Bürgerrechte & Polizei

Cilip 76
Nr. 3/2003

Polizei und Technik

US-Patriot-Act
Rechtshilfeübereinkommen mit den USA
Gutachten des MPI zur Telefonüberwachung

Herausgeber:
Institut für Bürgerrechte & öffentliche Sicherheit e.V.
Verlag: **Verlag CILIP**, Malteserstr. 74-100, 12249 Berlin
Redaktion, Gestaltung + Satz:
Heiner Busch (verantw.), Martina Kant, Norbert Pütter, Marion Knorr
Titelblattgestaltung: Martina Kant, Martin Hufner
Titelbild: Foto, Johannes Wartenweiler
Übersetzungen: Katrin McGauran
Druck: Kästner Druck GmbH
Berlin, Dezember 2003

Vertrieb: Verlag CILIP, c/o FU Berlin
Malteserstr. 74-100, 12249 Berlin
Tel.: (030) 838-70462
Fax: (030) 775 10 73
E-Mail: info@cilip.de
WWW: http://www.cilip.de
Personen: Einzelpreis 7,20 / Jahresabo (3 Hefte) 18,50
Institutionen: Einzelpreis 11,– / Jahresabo 32,50
Jahresabo zum Soli-Preis 25,– / Großer Soli-Preis 50,–
Alle Preise inkl. Porto · Das Abonnement verlängert sich automatisch um jeweils ein weiteres Jahr, wenn nicht bis 30.11. des Jahres gekündigt wird.

ISSN 0932-5409
Zitiervorschlag: Bürgerrechte & Polizei/CILIP 76 (3/2003)

Editorial
Heiner Busch 4

Polizei und Technik

Die Technologisierung der Polizei – eine Einleitung
Wolf-Dieter Narr 6

INPOL-neu: Informatisierung des polizeilichen Alltags
Heiner Busch 12

Digitalfunk – nicht nur eine Kostenfrage
Stephan Stolle 20

DNA-Identifizierung
Detlef Nogala 28

Biometrische Kontrollen nach dem 11. September
Jonathan P. Aus 36

Automatische Nummernschilderkennung
Daniel Boos 43

„Nicht-tödliche" Waffen für Kriege und Innere Einsätze
Olaf Arndt und David Artichouk 49

Rechtshilfe- und Auslieferungsabkommen mit den USA
Hartmut Wächtler 57

Anti-Terror-Gesetze in den USA
Clemens Arzt 65

Telekommunikationsüberwachung wissenschaftlich verharmlost
Norbert Pütter 73

Inland aktuell 85

Meldungen aus Europa 90

Chronologie
Marion Knorr 94

Literatur 103

Summaries 108

Editorial

von Heiner Busch

Als die deutsche Polizei in den 60er Jahren anfing, über die Einführung von Computern nachzudenken, hatte sie eine andere technische Revolution gerade erst zum Abschluss gebracht: die Motorisierung. Begonnen hatte sie Anfang der 20er Jahre mit dem Ziel, eine politische und soziale Revolution zu verhindern. Die Kasernierte Sicherheitspolizei (SIPO) war der erste Organisationsteil, der mit Kraftfahrzeugen ausgestattet wurde. Lastwagen – zunächst aus Militärbeständen übernommene – ermöglichten die schnelle Verlegung an „bedrohte und umkämpfte Orte" und lösten die hoch militarisierten SIPO-Truppen aus ihrer Abhängigkeit von der Eisenbahn. Im polizeilichen Alltag spielte das Auto noch lange keine bedeutende Rolle. Erst in den 50er Jahren ging man daran, neben den üblichen Fußstreifen zunächst versuchsweise motorisierte Funkstreifen einzurichten. Mit den Organisationsreformen der 70er Jahre verschwanden die Fußstreifen fast vollständig. Diese technische Revolution war definitiv abgeschlossen.

Rund 35 Jahre, nachdem die Elektronik ihren Einzug bei der Polizei begann, erleben wir einen ähnlichen Normalisierungsprozess. Mit INPOL-neu verabschiedet sich die Polizei von der Großrechnertechnologie. 270.000 PolizistInnen, so tönt es aus dem polizeilichen Blätterwald, werden Zug um Zug mit vernetzten PCs ausgestattet. Die Arbeit am Bildschirm ist nicht mehr nur für SpezialistInnen gedacht, sie soll zum Regelfall werden. Benutzerfreundlichkeit ist daher angesagt. Die Herauslösung der Information aus den Niederungen der polizeilichen Akten- und Fallbearbeitung, die sich die Protagonisten der polizeilichen Informationstechnik in den 70er Jahren erhofft hatten, scheint Jahrzehnte später Wirklichkeit zu werden. Arbeitsvorgänge, die wie der Vergleich von Fingerabdrücken früher Stunden in Anspruch nahmen, sind heute weitgehend automatisiert. Kfz-Kennzeichen lassen sich im Vorbeifahren lesen und mit polizeilichen Datenbeständen abgleichen. Biometrische Verfahren bringen die automatische Grenzkontrolle. Was aus polizeilicher Sicht als Rationalisierung und Vereinfachung der Poli-

zeiarbeit durch den Einsatz von Technik aussieht, stellt sich im Hinblick auf die Bürgerrechte als neue Bedrohungen dar. Das polizeiliche Kontrollpotential wächst, und in immer wieder neuen Varianten wird die Illusion genährt, dass eine technisch perfekt ausgerüstete Polizei den „Kampf gegen das Verbrechen" gewinnen könnte.

Der Weiterentwicklung der neuen Technologien scheinen keine Grenzen gesetzt. So „abgedreht" manche der neuen Instrumente erscheinen, so sehr bestimmen sie doch mittlerweile die Normalität sowohl der Polizei und der dort arbeitenden Individuen, als auch die der Bürgerinnen und Bürger, welche den neuen Formen der Kontrolle unterworfen sind. Polizeiliche Eingriffe erscheinen erst dann als bedrohlich, wenn sie weh tun. Die neuen Techniken kommen ohne Gewalt aus; mitunter versprechen sie auch den Kontrollierten Vorteile: An die Videokamera im Stadtbild hat man sich gewöhnt. Es ist bequemer, den maschinenlesbaren Personalausweis vorzuzeigen, als sich auf eine elend lange Diskussion mit einem kontrollierenden Beamten einzulassen. Die DNA-Analyse gehört als ständiger Bestandteil des abendlichen Fernsehkrimis zur Unterhaltung der Eltern. Und die Kinder spielen – dank Lego – den Großen Lauschangriff. Nicht nur in den Kinderzimmern werden die alten grün-weiß gestreiften Polizeiautos um die Überwachungsapparaturen erweitert. Der reale Polizeialltag in der Gegenwart wird vom Zusammenwirken der „handfesten" polizeilichen Ressourcen, d.h. den verschiedenen Formen unmittelbaren Zwangs, mit den fortgeschrittenen Techniken der Registrierung, Überwachung und Kontrolle bestimmt.

***

Die nächste Ausgabe von Bürgerrechte & Polizei/CILIP erscheint im Frühjahr. Sie wird sich im Schwerpunktteil mit der polizeilichen Statistik auseinandersetzen.

Heiner Busch ist Redakteur von Bürgerrechte & Polizei/CILIP.

Die Technologisierung der Polizei

... und ihre dringliche Politisierung

von Wolf-Dieter Narr

Seitdem die Polizei im 19. Jahrhundert aus dem Militär ‚ausgefällt' wurde, spielte ihre spezifische technische Ausstattung eine zentrale Rolle. Aus den informationellen und handfesten Techniken der Verbrechensbekämpfung, der Unruhe-Pazifizierung und der Strafverfolgung wurden seit Ende der 60er Jahre Technologien, die die Polizei selbst grundsätzlich veränderten.

Der Begriff Technologie beinhaltet bekanntlich mehr als eine bloße Sammlung einzelner technischer Instrumente mit jeweils eigener Gebrauchslogik. Sie verändert die Gebrauchsweise, den Gegenstand, für den sie gebraucht wird, und die Gebrauchenden selbst. Kurzum die gesellschaftlichen Herstellungs- und Umgangsformen wandeln sich insgesamt. Die Informations- und Kommunikationstechnologie hat dies seit den späten 60er Jahren offensichtlich getan. Das gilt für die Polizei in besonderem Maße. Seit der Ankunft von Kommissar Computer, wie es Anfang der 70er Jahre noch hieß, haben sich nicht nur die polizeilichen Instrumente gewandelt. Es änderte sich die Polizei – ihre Aufgaben, ihre Institutionen und ihre politischen Funktionen.

Großbritannien, dessen vertraute Bobby-Symbolik längst verblichen ist, spielte nicht zufällig eine kleine Vorreiterrolle in dem, was Carol Ackroyd u.a. „the New Technology of Repression" genannt haben. Hier begann mit dem Nordirland-Konflikt der sicherheitspolitisch-polizeiliche „technological fix", der sich rasch in der BRD und anderen europäischen Staaten ausbreitete.[1] Der Kontext, in dem diese Neue Technologie ausge-

1 Ackroyd, C. et al.: The Technology of Political Control, New York, London 1977; für die BRD s.a. Busch, H. u.a.: Die Polizei in der Bundesrepublik, Frankfurt/M. New York 1985

brütet wurde und den sie selbst mit produzierte, wurde hauptsächlich durch den Beginn einer neuen Globalisierungsstufe markiert, die sich seitdem durch ein spannungsreiches Quartett von Entgrenzung und neuer Vergrenzung, von ausschließender Konkurrenz und zusätzlichen Interdependenzen auszeichnet. Aktuell problemverschärfend wirkte über den regional begrenzten Nordirland-Konflikt hinaus der Vietnamkrieg und die auch in ihren Formen neuen Proteste, die er in Westeuropa und Nordamerika auslöste. Diese zeichneten sich dadurch aus, dass, wenn nicht „die Massen", so doch demokratisch gerichtete Gegenkräfte innerhalb und außerhalb der etablierten Institutionen als ernsthafte Akteure auf den Plan traten.

Das Thema „Polizei und Technik/Technologie" ist also nicht ganz so neu. Alarmismus bringt deshalb wenig. Zu oft schon wurde vor dem „totalen Überwachungsstaat" gewarnt – eine Klage, die sich verbraucht. Das Thema „Polizei und Technik/Technologie" ist zugleich ständig neu und brandaktuell. Neue technologische Entwicklungen werden – meist militärisch vorprobiert und initiiert – mit kürzer gewordenen Verzögerungen von den Polizeien rezipiert. Das an sich schon gesellschaftspolitisch hochgeladene Thema der Neuen Technologien und ihrer soziopolitischen und ökonomischen Bedeutung wird im Umkreis ihres polizeilichen Gebrauchs zum geradezu umfassenden Politikum. Hier werden Macht-, Herrschafts-, Kontroll-, Demokratie- und Menschenrechtsfragen mitentschieden.

Von den 70er Jahren zur Gegenwart

Während der 70er Jahre vollzog sich der „technological turn" der Polizei(en). Materialreich beschrieben Carol Ackroyd u.a. 1977 das technologische Gebrauchs-Kontinuum zwischen Militär und Polizei. Angefangen von Counter Insurgency-Technologien und -maßnahmen – der Massenkontrolle, des Umgangs mit Großdemonstrationen – bis hin zu neuen Formen der Sammlung, Speicherung, Weitergabe von Informationen und ihrer mehr oder minder vermittelten exekutiv-polizeilichen Verwendung. Was jedoch in den 70er Jahren selbst bei der „Mr. Computer" genannten Person, dem BKA-Chef des anti-terroristischen Kampfes Horst Herold, noch wirkte, als gehe jemand gernegroß in prätentiösen, technologisch gespornten Sicherheitsstiefeln, ist heute längst zum polizeilichen Alltag geworden. PC- und Internettechnik haben nicht nur die Polizei von oben nach unten nahezu restlos durchdrungen. Informations- und Kommuni-

kationstechnologien, die sich seit 30 Jahren immer rasanter, feiner und umfassender entwickeln, haben Umfang und Intensität der Kontrolle quantitativ und qualitativ so verändert, dass eine signifikante Kehre von der Taten und Tätern nachhinkenden Repression zur präventiven Vorfeldkontrolle stattgefunden hat. Ihr wird potentiell jede und jeder ‚unschuldige' BürgerIn unterworfen. Fremde an erster Stelle. Präventive Repression, das, was man militärisch den „preemptive strike" nennt, ist polizeilich längst Normalverhältnis.

Die Liste all der polizeilich zuhandenen Technologien, die Steve Wright von der Omega Foundation 1998 für das Europäische Parlament aufgelistet, beschrieben, knapp kommentiert und – mit eher hilflosen – demokratischen Umgangs- und Kontrollvorschlägen versehen hat,[2] unterscheidet sich beträchtlich von der technologischen Maßnahmen- und Aufgabenliste, die gute 20 Jahre zuvor von Ackroyd und Mitarbeitern apostrophiert worden ist. Schon einleitend spricht Wright von einer „global surveillance machinery".

Zu dieser zählen Maßnahmen und Instrumente, die aus dem „antiterroristischen Kampf" à la Nordirland oder BRD der 70er Jahre im Prinzip bekannt sind: massenhafte Erfassung, pauschale Kontrollstellen für Autos und Personen, „nicht tödliche" Waffen. Im Unterschied zu den 70er Jahren ist aber die Kapazität der Speichermedien erheblich größer. Fingerabdrücke werden heute nicht mehr manuell verglichen, sondern durch Automatische Fingerabdruck-Identifizierungssysteme. Kontrollstellen beruhen auf einem nicht sichtbaren technischen Apparat, der den Vorgang der Kontrolle beschleunigt und effektiviert. Und das ständig um neue Erfindungen erweiterte Repertoire der „Crowd-control"-Waffen stellt jeden Science-Fiction-Roman in den Schatten.

Hierher gehören jedoch auch neue Versionen der Videoüberwachung: Sie ermöglichen es nicht nur, die Bewegungen einer Person quer durch ganze Gebäudekomplexe oder gar Innenstädte am Bildschirm nach zu verfolgen. Sie nutzen die Synergien anderer Neuer Technologien – Mustererkennungs- oder biometrischen Verfahren – und automatisieren die Kontrolle von Fahrzeugen oder Personen.

---

2 Wright, S.: An Appraisal of Technologies of Political Control. Working Document, Luxembourg 1998 (European Parliament, Scientific and Technological Options Assessment (STOA), Working Document PE 166499; http://jya.com/stoa-atpc.htm); für einen vergleichsweise frühen Überblick vgl. auch Nogala, D.: Polizei, avancierte Technik und soziale Kontrolle, Pfaffenweiler 1989

Und hierher gehört schließlich die technologische Aufrüstung gegen „unerwünschte“ Ausländer, gegen Asyl Suchende zumal, die zu den „Versuchskaninchen“ neuer Sicherheitstechnologien geworden sind und die nicht in die technologisch viel armierte, notfalls mit neuen Lagern umrahmte Festung Europa hinein gelassen werden sollen: von diversen Spähgerätschaften zur Grenz-„Sicherung“ bis hin zu Chipkarten, welche die Kontrolle aller möglichen Lebensäußerungen erlauben.

Rechtliche Wurzeln in der Luft

So wichtig es jedoch ist, all der sicherheitstechnologischen Entwicklung auf der aktuellen Spur zu bleiben, die sich eigendynamisch beschleunigt, so schwer lassen sich zum einen die allgemein politischen und die spezifisch polizeilichen Folgen genau fassen; so schwierig ist es zum anderen, die ökonomisch und politisch treibenden Faktoren einer technologisch ver-rückt wirkenden Entwicklung systematisch plausibel auszumachen. Geht es doch nicht an, statt triftiger Analyse allein auf den „Sicherheitswahn“ zu verweisen, der überall Wühlmäuse und Verbrecher am Werke sieht. Nur eines ist im Zusammenhang von „Polizei und Bürgerrechten“ – nüchtern gesprochen – erschreckend klar: Alle rechtlichen und alle repräsentativ-demokratisch institutionalisierten Kontrollvorkehrungen wirken wie Wurzeln in der Luft – stark ausgestreckt und ausgereckt, indes gänzlich ohne jeden Boden, der Kontrolle erst erlaubte.

Auf den ersten Blick gilt ohne Frage: Der Ausbau des technologischen Sicherheitsstaats und seiner internationalen Einrichtungen stärkt die Exekutive. Wer aber „ist“ die gestärkte Exekutive? Ist es etwa die politische (gewählte und wenigstens formell verantwortliche) Klasse? Gewiss: die technologischen Sicherheitsperfektionen stärken deren Herrschaft. Indes, die „politische Klasse“ vermag die technologisch noch unübersichtlicher, noch hermetischer gewordenen Apparate nicht zu kontrollieren. Ist es das letztlich legislativ gesatzte Recht und die Recht kontrollierend anwendende Justiz? Nein, abgesehen von der primär staatstragenden Rolle der Dritten Gewalt wird das Recht mit unbestimmten Rechtsbegriffen, Gleitklauseln aller Art, insbesondere seit der präventiven, technologisch ermöglichten Kehre so ausgehöhlt, dass fast alles rechtens ist, was polizeilich technologisch gemacht werden kann. Die Legislativen können nur noch staunen, was sie verabschiedet haben. Die Bürger können sich Prozesse ersparen. Das Recht ist geradezu sicherheitstechnologisch aufgehoben (also beseitigt und technikgemäß bewahrt in einem).

Die Herrschaftsdienlichkeit der sich mehrfach überlagernden, vielfingrigen technologischen Sicherheitsnetze lässt sich kaum noch institutionell, noch viel weniger personal zuordnen, so sehr Personen und Institutionen davon profitieren. Diese Netze dienen in einer nur technologisch erreichbaren Weite und Tiefe dem System kapitalistischer Herrschaft jenseits aller liberaldemokratischen Verfassungsgarnierungen.

Dementsprechend versagen auch die immer widersprüchlichen staatlichen Kontroll- und bürgerlichen Schutzvorkehrungen. Die ausgrenzenden Sicherheitstechnologien kennen selbst keine Grenzen. In Zeiten neoliberaler Globalisierung überwuchern die exekutivisch vertäuten Sicherheitstechnologien alle Grenzen. Die europäischen und die europäisch-amerikanischen Zusammenarbeits-, Austauschformen und immer noch Rechtshilfe genannten Abkommen demonstrieren diesen zusätzlichen „staatsbürgerlichen" Kontrollverlust.

Am meisten fällt auf und irritiert eingestandenermaßen, in welchem Ausmaße die neuen Sicherheitstechnologien geradezu zu Wonnen bürgerlicher Gewöhnlichkeit werden. An der ausufernden Videoüberwachung im Kontinuum zwischen privatem und öffentlichem Sicherheitsinteresse kann man diese Gewöhnung am leichtesten fassen. Dass dem so ist, hängt mit der materiell schwer fassbaren Wirkung der Technologien zusammen; auch damit, dass technologische Vorkehrungen und Praktiken zum bürgerlichen Alltag geworden sind. Eine Art tägliche Reality-Fernsehshow.

Antiquiertheit der Menschenrechte

Angesichts des technisch verändernden, in alle Poren dringenden ‚Überflusses' ist Günther Anders' technik-kritische Beobachtung der „Antiquiertheit des Menschen" aktueller denn je. Im Zeichen der Sicherheitstechnologien wirken in jedem Fall die Menschenrechte antiquiert. Das Wort „Unversehrtheit" erscheint vor dem Hintergrund all dieser technologischen Feingriffe als ein zu grober Begriff von Integrität, an dem sich deren Durchlöcherungen neuer Art nicht mehr messen lassen. Die aus Techniken zu Technologien gewordenen Späh-, Informationssammel- und Eingriffsinstrumente wirken zum einen ungleich sublimer. Zum anderen trennen sie alle soziogenetischen Zusammenhänge und stellen einen anderen Triumph der Vereinzelung dar (im ideologischen Jargon der Gegenwart: der Individualisierung).

Angesichts der an dieser Stelle nur lückenhaft darstellbaren Merkmale der neuen Sicherheitstechnologien wird erfahrbar, wie wenig die Menschenrechte dazu taugen, ihre ebenso sublime wie radikale Verletzung auch nur anzuzeigen, sprich: subjektiv und kollektiv, also politisch erfahrbar zu machen. Das staatliche Gewaltmonopol, seine hauptsächlichen Instanzen und Aktivitäten waren bis in jüngste Zeit vergleichsweise leicht zu fassen. Gewaltzugriffe auf den menschlichen Körper entgegen dem Urrecht auf Integrität, Einbrüche in die Wohnung u.v.a. waren jedenfalls mühelos erkennbar. In diesem Sinne war staatliche (anders auch kapitalistische) Politik früher ungleich „biopolitischer" als heute, da dieser Begriff zu einem neuen Modeausdruck geworden ist. Mit den neuen Sicherheitstechnologien wird zwar tief in den Körper der Menschen eingegriffen. Diese Feingriffe sublim totaler Körperkontrolle bemerken wir jedoch erst, wenn das Gewaltmonopol in seiner „herkömmlichen Form" auftritt und den Körper des als möglichen Täter erkannten Individuums höchst traditionell festnimmt. Will man in Sachen Kontrolle der technologischen Kontrolleure nicht von vornherein verzweifeln, kommt es also entscheidend darauf an, die Menschenrechte ungleich materieller und differenzierter zu fassen. Damit die sublimen Feingriffe spürbar, messbar und kommunizierbar werden.

In Sachen neoliberal-etatistischer Sicherheit im Zeitalter ihrer technologischen (Re-)Produktion kommt es entgegen der entpolitisierenden Tendenz, die mit der „Technokratisierung der Sicherheit" schattengleich einhergeht, darauf an, diese neuen Sicherheitstechnologien in ihrer antisozialen, anti-menschenrechtlichen Logik ständig neu in ihren Herrschaftssinnen aufzudecken. Darum gilt die Parole der Politisierung der Sicherheitstechnologien an erster Stelle.

Wolf-Dieter Narr lehrt Politikwissenschaft an der FU Berlin und ist Mitherausgeber von Bürgerrechte & Polizei/CILIP.

INPOL-neu

Informatisierung des polizeilichen Alltags

von Heiner Busch

Nach über zehn Jahren Planungsdiskussion und Entwicklungsarbeiten, einem weitgehenden Scheitern der ursprünglichen Pläne und einem bescheideneren Neuanfang ging am 18. August 2003 die erste Stufe von INPOL-neu in Betrieb.

Als die ersten 35 Terminals des alten INPOL-Systems im Herbst 1972 ans Netz gingen, schien für die Polizei eine neue Ära anzubrechen. „Kommissar Computer" wurde von seinen polizeilichen Kollegen mit Jubel begrüßt. Im August 2003, beim Start von INPOL-neu, mochte dagegen keine rechte Begeisterung aufkommen. Eher war man erleichtert, dass es mit dem neuen System doch noch geklappt hatte, bevor im Jahr 2004 die Wartungsvereinbarungen für die Software des alten abgelaufen wären, bevor die letzten internen Spezialisten in Pension gingen und ohne dass das Fahndungssystem zusammenbrach.

Begonnen hatte die Geschichte von INPOL-neu mit einem Beschluss des Arbeitskreises II (AK II) der Innenministerkonferenz, der im Januar 1992 den Auftrag für ein fachliches Grobkonzept erteilte. Noch im November desselben Jahres präsentierte ein Projektteam von zwölf Fachleuten aus Bund und Ländern den verlangten Bericht, den der AK II nach einer Überarbeitung im September 1993 guthieß. 1995 folgte das technische Grobkonzept sowie eine Aufwandsstudie. Das eigentliche Projekt, für dessen Realisierung man drei Jahre angesetzt hatte, startete aber nicht wie vorgesehen im Oktober 1995, sondern ein ganzes Jahr später.[1]

1 Zentralstelle INPOL-neu: Projekt INPOL-neu. Informationen zu Historie, Sachstand und Planung, Wiesbaden, 28.8.1997

Ab 1998 wurde programmiert. Im selben Jahr bemerkten diverse Bundesländer, dass sie mit den Vorleistungen für den Anschluss ihrer Landessysteme an INPOL-neu im Verzug waren.[2] INPOL-neu ging weder am 1. Januar 2000 noch am 15. April 2001 in Betrieb. Ein Testlauf im April 2001 führte zu einem Totalabsturz. Im Januar 2002 entschloss sich die Innenministerkonferenz zu einem bescheideneren Neubeginn. Insgesamt sind über 50 Millionen Euro in den Sand gesetzt worden, argumentieren die KritikerInnen. Nicht ganz, rechtfertigt sich das Bundesinnenministerium. Man habe einige Komponenten der ursprünglichen Planung für INPOL-neu übernehmen können.[3]

INPOL-alt – kurz vor dem Kollaps

Unstrittig ist dagegen, dass das INPOL-System in seiner alten Form so nicht mehr weiterbetrieben werden konnte. Das Konzept dafür stammte von Anfang der 70er Jahre und basierte dementsprechend auf einer mittlerweile veralteten Großrechnertechnologie. Zwanzig Jahre danach war der Wartungsaufwand personell und finanziell enorm, vergleichsweise billige Standardsoftware ließ sich nicht integrieren.

Weil die Länder mit Anlagen verschiedener Herstellerfirmen arbeiteten, war die INPOL-„Architektur“ von Anfang an äußerst kompliziert. Für die Hälfte der Bundesländer hieß das noch in den 90er Jahren, dass die polizeilichen NutzerInnen via Terminal – unter Umgehung ihres Landessystems – unmittelbar auf die Zentrale Datenverarbeitungsanlage des BKA zugreifen mussten, weil ein eigentlicher Verbund zwischen Landes- und BKA-System, ein so genannter Rechner-Rechner-Verbund, nicht möglich war.

Auch hinsichtlich Funktionen und Dateninhalten war INPOL-alt kein System aus einem Guss. In den 90er Jahren bestand es aus insgesamt 27 verschiedenen Anwendungen. Über gemeinsame Grunddaten verknüpft waren allerdings nur die „Personendateien“: die Personenfahndung, der Kriminalaktennachweis (KAN), die Haftdatei und schließlich die Erkennungsdienstdatei. Eine einzige Abfrage ergab hier, ob eine Person zur Fahndung oder Beobachtung ausgeschrieben war, ob und wo Unterlagen über INPOL-relevante, d.h. überregional bedeutende und schwere Straf-

2 Sehr, P.: INPOL-neu: System mit Merkmalen eines extremen Wandels, in: Kriminalistik 1999, H. 8, S. 532-536 (536)

3 die tageszeitung v. 2.1.2002 und 20.8.2003

taten vorhanden waren, oder ob die Person einen Eintrag in der Fingerabdruckdatei AFIS oder ab 1998 in der DNA-Datei hatte.
Die restlichen Anwendungen waren jedoch von den Personendateien abgekoppelt. Das galt sowohl für die Falldateien (u.a. Falldatei Rauschgift) als auch für die seit den 80er Jahren entwickelten PIOS- und SPUDOK-Anwendungen, die jeweils nur Spezialabteilungen (Staatsschutz, Drogen, Organisierte Kriminalität) oder Sonderkommissionen zur Verfügung standen.

Die Projektgruppe INPOL-neu beklagte denn auch als wesentlichen Mangel des alten Systems den Zwang zur Mehrfacherfassung. Die SachbearbeiterInnen müssten mit derselben Information über eine Person oder einen Fall nicht nur das jeweilige Landessystem, sondern zusätzlich die verschiedensten „Töpfe" von INPOL bedienen. Komplizierte Erfassungscodes und die allgemeine Benutzerunfreundlichkeit hätten dazu geführt, „dass sich Spezialisten in den Dienststellen herausbilden ... und nicht mehr der Sachbearbeiter die Recherchen mit seinem Fachwissen durchführt, sondern eine Erfassungskraft, weil nur sie die Ein- und Ausgabemodalitäten kennt."[4] Die Erfassung erfolgte denn auch oft nur selektiv, viele Informationen seien gar nicht weitergeleitet worden. Im Bereich des allgemeinen Kriminalpolizeilichen Meldedienstes, so klagte der BKA-Mann Peter Sehr vor zwei Jahren, würden maximal 23 Prozent der an das BKA mitzuteilenden Straftaten gemeldet. „Zutreffende oder gar strategische Aussagen auf der Basis dieser Anlieferungsmengen machen zu wollen, grenzt an polizeiliche Kaffeesatzleserei."[5]

INPOL-neu: die Planungen

Die Projektgruppe INPOL-neu entwarf ihr Konzept als Gegenbild der skizzierten Mängel des alten Systems. Sie hatte dabei nicht nur eine Neuorganisation des zentralen von Bund und Ländern gemeinsam genutzten Bereichs, also des eigentlichen INPOL-Systems, im Auge, sondern stellte auch Vorbedingungen für die Landessysteme (bzw. die eigenen Systeme des BKA und des Bundesgrenzschutzes). Alle an INPOL Beteiligten sollten neu über eine einzige gemeinsame Schnittstelle an das gemeinsame

4 Projektgruppe INPOL-neu: Abschlussbericht für die Phase „Grobes Fachkonzept", Wiesbaden November 1992, S. 73

5 Sehr, P.: INPOL-neu – Aufbruch zu einer neuen Generation der polizeilichen Datenverarbeitung, in: der kriminalist 2001, H. 2, S. 60-63 (60)

System angeschlossen werden. „Mit der Kommunikationsschnittstelle“, so hieß es im Sachstandsbericht von 1997, „beginnt und endet das System INPOL-neu. Es ist damit eindeutig von den Landessystemen sowie denen des BKA und des BGS abgegrenzt.“[6]

Die Länder waren damit verantwortlich für die Erneuerung ihrer eigenen Datenverarbeitung. Sie sollten zweierlei Systeme aufbauen: zum einen „Landesdatenhaltungssysteme“ für jene Informationen, die nicht in INPOL gespeichert werden dürfen, weil sie weder überregional relevante noch schwere Straftaten betreffen; zum andern sogenannte „Vorgangsbearbeitungssysteme“, in denen alle polizeilich relevanten Ereignisse – „Vorgänge“ – erfasst, verwaltet, bearbeitet, abgelegt oder an andere Stellen weitergeleitet würden: Anzeigen, Berichte, Protokolle, durchgeführte Maßnahmen etc.

Mit dem Aufbau solcher Systeme werden die Arbeitsplätze sämtlicher polizeilichen SachbearbeiterInnen zu Computerarbeitsplätzen. Aus dem an ihrem Arbeitsplatz vorfindlichen Vorgangsbearbeitungssystem heraus können die BeamtInnen je nach ihrer Berechtigung auf sämtliche Polizeidateien zugreifen oder darin surfen – vom Landesdatenhaltungssystem über INPOL-neu bis hin zum Schengener Informationssystem. Auch die Verbindung zum Ausländerzentralregister und zum Zentralen Verkehrsinformationssystem sollte von hier aus möglich sein.

Die Vorgangsbearbeitung wird damit zum Sockel der polizeilichen Datenverarbeitung. Weil die Daten in der Bearbeitung von Fällen an der polizeilichen Basis anfallen, sollten sie auch hier erfasst und von dort an die Landesebene oder an INPOL-neu weitergeleitet werden. Die Antwort auf die Frage, ob eine Information zentral zu speichern ist, wollten die PlanerInnen von INPOL-neu aber nicht den jeweiligen SachbearbeiterInnen alleine überlassen. In „Muss“-Fällen sollte entsprechend eines Deliktkatalogs automatisch eine Erfassung in INPOL erfolgen. Nur bei „Regel“- und „Kann“-Fällen hätten die Eingebenden noch Entscheidungsmöglichkeiten gehabt.

Um den vollständigen Überblick über die kriminelle Karriere einer Person zu erhalten, verlangte das „fachliche Konzept“ von INPOL-neu ferner die Durchbrechung der bis dahin geltenden Aufteilung von Landes- und Bundesdaten an einem wichtigen Punkt: Wenn eine Person einer INPOL-relevanten Straftat beschuldigt wird, sollten nun auch alle

6 Zentralstelle INPOL-neu a.a.O. (Fn. 1), S. 4

anderen ihr zugeordneten Delikte zentral erfasst werden, auch wenn es sich dabei um Bagatellen handelt.
Beim Aufbau von INPOL-neu wollte die Projektgruppe den Wildwuchs des alten Systems von Anfang an vermeiden. An die Stelle der verschiedenen Anwendungen, in denen bestimmte Daten jeweils neu und damit mehrfach zu erfassen waren, sollte nun ein Datenpool treten, dessen zentrales Prinzip die „Einmalerfassung" sein sollte. Zusammenhängende Informationen über Personen, Fälle, Sachen etc. sollte das System automatisch zusammenführen. Die Falldaten sollten für alle Deliktsbereiche einheitlich erfasst werden. Deliktspezifische Falldateien, Meldedienste oder PIOS-Anwendungen sollten zugunsten einer „ganzheitlichen Sichtweise" verschwinden. Das Konzept für INPOL-neu versprach einfache Möglichkeiten des Abfragens, der freien Recherche, der grafischen und tabellarischen Aufbereitung, zusätzliche Bild- und Videodaten und vor allem eine rundum verbesserte Auswertung. INPOL-neu sollte „sozusagen eine Super-DOK oder ein Gigant-PIOS" sein.[7]

Nach den Vorstellungen der PlanerInnen sollte INPOL-neu jedoch nicht nur operative, d.h. fallbezogene Auswertungsmöglichkeiten bieten, sondern auch ein „Führungsinformationssystem" für strategische Analysen sein: für die Erstellung der Kriminalstatistik, die eine Ausgangsstatistik ist, also den Abschluss eines polizeilichen Ermittlungsverfahrens registriert, für eine polizeiliche Eingangsstatistik sowie für Lagebilder. Für diese Zwecke sollten nicht nur die INPOL-relevanten Straftaten gemeldet werden, sondern – wenn auch in anonymisierter Form – auch sämtliche anderen.

INPOL-neu: die Realität

„Nicht seriös kalkulierbare Zeit- und Kostenpläne", attestiert Holger Gadorosi, Gesamtprojektleiter INPOL-neu den bis Ende 2001 verfolgten Plänen. Der Konzeption nach hätten sämtliche Länder und der BGS innerhalb einer kurzen Zeitspanne INPOL-neu einführen sollen. „Dieser Ansatz war deshalb notwendig, weil das geplante INPOL-neu-System inkompatibel zu den aktuellen Ländersystemen war."[8] Die Länder konnten dieser Anforderung aber nur zum Teil entsprechen. Daran konnte auch die zwischenzeitlich eingerichtete Arbeitsgruppe INPOL-Land

7 Sehr a.a.O. (Fn. 5), S. 60
8 Gadorosi, H.: INPOL-neu, in: Kriminalistik 2003, H. 5, S. 402-409 (409)

(AGIL) nichts ändern. Die Folgerung daraus war die Aufgabe des „Geleitzugs“, des Prinzips der gleichzeitigen Einführung also, zugunsten einer Stufenplanung. Die im August 2003 eingeführte „Version 4“ von INPOL ist „abwärtskompatibel“ zu den alten Ländersystemen. Erst wenn sämtliche Bundesländer zu dieser neuen Version aufgeschlossen haben, wird sie abgelöst durch eine „Version 5“, die dann den vorläufigen Endausbau von INPOL-neu darstellen soll. Das Führungsinformationssystem, jetzt dispositives System genannt, wird erst in dieser Version folgen. In der Version 4 enthält INPOL drei Untersysteme: INPOL-Z, F und K.

INPOL-Z (wie zentral) ist ein allgemeines Fahndungs- und Auskunftssystem und bedient laut Gadorosi die Bedürfnisse der großen Mehrheit der PolizeibeamtInnen. Aufgrund der benutzerfreundlichen Internet-Technologie, einfacher Auskunftsmasken und der Zugriffsmöglichkeit aus dem Vorgangsbearbeitungssystem heraus erwartet der Gesamtprojektleiter eine massive Steigerung der Zahl der Abfragen.

Personen- und Sachdaten enthalten jeweils die Fallgrunddaten „beispielsweise Tatort und -zeit, Deliktschlüssel, Aktenzeichen sowie sachbearbeitende Dienststelle“. Über die Fallangaben können unter den betreffenden Personen und zwischen den Personen und Sachen „Beziehungsgeflechte“ hergestellt werden. Personendaten enthalten neu auch Fotos. „Die bestehende Lichtbildersammlung des BKA wird sukzessive in das System übernommen.“[9] Um das Risiko eines Totalausfalls der Fahndung zu vermeiden, werden sämtliche Fahndungsdaten anders als ursprünglich geplant nach wie vor sowohl im jeweiligen Landessystem als auch in INPOL-Bund gespeichert.

INPOL-F (wie Fall) ersetzt die bisherigen PIOS-, DOK-, SPUDOK- und Falldateien. Gedacht ist dieses System in erster Linie für die AnwenderInnen in Landeskriminalämtern und BKA. Die Datensätze enthalten Freitextfelder, in denen sich nicht nur Text, sondern auch „multimediale Inhalte“ speichern lassen – von der Fax-Kopie bis hin zu Fotos und Videos. „Alle Informationsobjekte ... lassen sich über beliebige Beziehungen verknüpfen und in späteren Analysen auswerten.“[10]

Im Unterschied zu den früheren Planungen hat man jedoch keine deliktübergreifende Falldatei aufgebaut, sondern es zumindest in der Version 4 bei verschiedenen abgetrennten Anwendungen belassen. Falldaten

9 ebd., S. 406
10 ebd.

„im Bereich organisierter und politisch motivierter Kriminalität“ hätten eine „hohe Sensibilität“ und sollen daher weiterhin nur den MitarbeiterInnen der zuständigen Spezialdienststellen zugänglich sein. Aus den selben Gründen gaben die INPOL-MacherInnen auch das Prinzip der Einmalerfassung auf. Wenn eine Person Gegenstand (geheimer) Vorfeldermittlungen ist, darf es nicht passieren, dass ein kleiner Sachbearbeiter davon erfährt, nur weil er in einer „leichten Straftat“ gegen dieselbe Person ermittelt. Eine automatische Zusammenführung von Datenbeständen zur selben Person musste deshalb verhindert werden.

Statt der delikt-unspezifischen Speicherung bietet die jetzige Version von INPOL-neu eine anwendungsübergreifende Suche. „Dabei werden alle Datenbestände aller INPOL-Falldateien nach Treffern durchsucht, für die der Anwender berechtigt ist.“[11]

POLAS und ComVor

INPOL-K (wie Kommunikation) regelt schließlich die Schnittstellen zwischen dem Bundessystem und den Länderkomponenten. Die Länder können entweder eigene Systeme aufbauen oder das vom BKA angebotene POLAS übernehmen, das zunächst in Hamburg entwickelt und dann in Hessen angepasst wurde. Zusammen mit der Computer-unterstützten Vorgangsbearbeitung (ComVor) ergibt sich eine „völlig neue Infrastruktur zur Datenverarbeitung“.[12] Die Schreibmaschine hat ausgedient und wird vollends durch den vernetzten PC ersetzt, mit dem alle SachbearbeiterInnen ausgerüstet sind und von dem aus sie auch auf POLAS und INPOL zugreifen können. Die Reichweite der Zugriffsberechtigung ist individuell – auf einer Chipkarte (Hamburg) oder durch einen PIN-Code (Hessen) – festgelegt.

Für die diversen polizeilichen „Vorgänge“ hält ComVor Formularvorlagen bereit, die mithilfe üblicher Textverarbeitungsprogramme auszufüllen sind. Ein Teil der Formulardaten wird automatisch in einen Index, das Tagebuch, übertragen, das u.a. der internen Zuweisung von Arbeiten bzw. der Übernahme von „Vorgängen“ durch andere BeamtInnen dient. Bei einer Straftat sind das neben Tatort und -zeit auch Angaben zu den beteiligten Personen und ihrer Rolle als Beschuldigte, Ge-

11 ebd.

12 Der Hamburgische Datenschutzbeauftragte: 18. Tätigkeitsbericht 2000/2001, Hamburg 2002, S. 141-144 (141); s.a. den 17. Tätigkeitsbericht, Hamburg 2000, S. 85-92

schädigte, Anzeigende oder ZeugInnen. Während POLAS und INPOL nur die Daten der Verdächtigen oder Beschuldigten enthalten, sind im Tagebuch auch alle anderen Personen, die im Zusammenhang mit einer Straftat auftauchen recherchierbar – und zwar neu für alle SachbearbeiterInnen der jeweiligen Landespolizei.

Den Zugriff auf die eigentlichen Vorgänge selbst haben zunächst nur der oder die SachbearbeiterIn sowie die Vorgesetzten. „Mitarbeiter, die den Vorgang angelegt haben, können diesen an andere zuständige Dienststellen (z.B. vom Polizeirevier an das Kriminalkommissariat oder das Landeskriminalamt) weiterleiten“ oder KollegInnen zum Zugriff berechtigen. Die Vorgänge können für ein Jahr in ComVor archiviert werden.

Über die Speicherung im Landesdatenhaltungssystem POLAS oder in INPOL entscheidet in Hessen ein Analyst. Er legt zugleich die Speicherungsdauer und gegebenenfalls personengebundene Hinweise fest. Die ursprünglich geplante automatische Speicherung von Muss-Fällen in INPOL-neu wurde aufgegeben. Mit ihrer Kritik an der INPOL-Erfassung der ganzen „kriminellen Karriere“ einer Person – einschließlich der Bagatellen – sind die Datenschutzbeauftragten jedoch gescheitert.

Nicht ohne Folgen

Die hochfliegenden Pläne für INPOL-neu, mit denen die Polizei ein Jahrzehnt lang hantiert hat, mögen sich zwar erheblich reduziert haben. INPOL-neu und die damit zusammenhängenden Veränderungen auf Landesebene sind trotzdem nicht bedeutungslos. Während INPOL-alt den Arbeitsalltag der großen Mehrheit der PolizeibeamtInnen nicht antastete, durchdringt die automatisierte Datenverarbeitung nun die gesamte polizeiliche Organisation.

Die im Zuge des Neuanfangs 2002 veränderte „fachliche“ Konzeption verschafft dabei den ehernen Grundsätzen der Polizeiorganisation wieder Geltung: Geheim zu haltende Informationen bleiben bei den geheim arbeitenden Spezialdienststellen. Die unteren Ränge sollen zwar möglichst viele Informationen nach oben liefern, sie kommen aber weiterhin nur an allgemeine Auskünfte und in jedem Falle an Fahndungsnotierungen heran, deren Umsetzung man von ihnen erwartet.

Rechnung ohne Wirt

Digitalfunk – nicht nur eine Kostenfrage

von Stephan Stolle

Der heutige Analog-Sprechfunk sei veraltet, heißt es seit Anfang der 90er Jahre. Die „Behörden und Organisationen mit Sicherheitsaufgaben“ (BOS) – Polizei, Zoll, Feuerwehren, Rettungsdienste und Katastrophenschutz – wollen auf Digital-Funk umsteigen.

Seit über 30 Jahren kommen Polizei- und Rettungskräfte mit ihrem analogen Funk bestens zurecht. Die Kommunikation, die im Wesentlichen über zwei UKW-Bänder (4m und 2m) verläuft, hat sich durch den technischen Fortschritt ständig verbessert und wurde immer weniger störanfällig. Die allgemeine Miniaturisierung der Bauteile führte im Laufe der Zeit zu handlichen, robusten Geräten, die in hunderttausendfachen Stückzahlen leitstellenvermittelte Verständigung (Dispatching) ermöglichen. Strecken von einem bis 50 km oder (relaisvermittelt) über hunderte Kilometer werden bewältigt.

Der Analog-Funk erfüllt alle geforderten Aufgaben: das Führen von Kräften im mobilen Einsatz über Leitstellen, den Einbezug von Rettungs- und Polizeihubschraubern in das Netz, die Bildung funktionaler Gruppen und die freie „Gerät zu Gerät“-Kommunikation. Deutschland stellte durch ein System verschiedener DIN-Normierungen frühzeitig sicher, dass ein gleichbleibend hoher Qualitätsstandard gewahrt blieb. Ein Parallelsystem für Aus- und Fortbildung ermöglichte seit den 70er Jahren das Berufsbild des Leitstellenfunkers und stellte damit die Bedienungssicherheit auf Personalseite sicher.[1] Zwar mussten die bundesweit festgelegten Frequenzpläne und Kanalzuweisungen 1974 überarbeitet werden, weil die Gebietsreform jener Jahre die Gemeinde-, Kreis- und Bezirksgrenzen und

1 Sprechfunkdienst. BOS-Dienstvorschrift (PDV/DV 810.3), Stuttgart 1983

damit die Einteilung des so genannten Versorgungsgebietes verändert hatte.[2] Auch der Vertrag „Funktechnische Anpassung/Ost“, mit dem 1992 das „Beitrittsgebiet“ dem bundesrepublikanischen Standard angepasst wurde, brachte neue Frequenzzuweisungen sowie umfangreiche (und kostspielige) Geräteanschaffungen.[3] Ernsthafte Probleme wurden jedoch nicht berichtet.

Für Standardmeldungen (Abfahrt, Rückfahrt, angekommen usw.) gibt es inzwischen das Funkmeldesystem (FMS) und zur Alarmierung Fünf-Ton-Melodie-Folgen.[4] Der Analog-Funk ist zwar nicht grundsätzlich abhörsicher, aber die Einführung von taktischen (ab 1978) und technischen Verschleierungsmöglichkeiten („Zerhacker“) erschwert unbefugtes Mithören.[5]

Eine Übertragung von Bildern und Daten ist beim Analog-Funk ebenso wenig möglich wie die unmittelbare Abfrage von polizeilichen Datenbanken oder die direkte Einwahl ins Telefonnetz. Ferner wird mangelnde Frequenzökonomie und generell „veraltete Technik“ bemängelt. Angeblich stellt gar die Industrie die Produktion von Geräten und Ersatzteilen in absehbarer Zeit ein.

Mit Schengen ins digitale Zeitalter

Mit der Schengen-Kooperation bahnte sich eine neuerliche Veränderung im polizeilichen Funkwesen an. Das 1990 unterzeichnete Schengener Durchführungsübereinkommen (SDÜ) sieht nicht nur den Abbau der Kontrollen an den Binnengrenzen, sondern als „Ausgleichsmaßnahme“ diverse grenzüberschreitende Methoden vor, die ohne eine ebenfalls grenzüberschreitende Kommunikation zumindest erschwert wären. „Insbesondere im Hinblick auf die rechtzeitige Übermittlung von Informationen im Zusammenhang mit der grenzüberschreitenden Observation und Nacheile“ sieht deshalb Art. 44 Abs. 1 des Abkommens vor, kurzfristig „direkte Telefon-, Funk-, Telex- und andere Verbindungen“ in den Grenzgebieten einzurichten. In einem 20 km breiten deutsch-niederländischen Grenzstreifen entstand in der Folge das KTS-Netz

2 www.angelfire.com/realm/dschon/province/DEU-NI-alt.html
3 BT-Drs. 12/950 v. 5.7.1991
4 Plath, H.: Funkmeldesystem FMS – Funk ohne Worte, in: BOS-Funk 2 (Booklet 7), Burgdorf 1998; Marten, M.: BOS-Funk, Bd. 1, Meckenheim 1998, S. 204
5 Marten a.a.O. (Fn. 4) S. 122-124; www.funkmeldesystem.de/bos-funk.php

(Kortje Termijn Schengen), das die Leitstellen beider Länder verbindet und über die Leitstellen auch den direkten Funkkontakt zwischen den Einsatzkräften ermöglicht.

„Über diese Sofortmaßnahmen hinaus“, so heißt es in Absatz 2 desselben Artikels, sollten die Vertragsstaaten die „Koordinierung ihrer Programme für den Erwerb von Kommunikationsgeräten“ prüfen – und zwar „mit dem Ziel der Einrichtung genormter und kompatibler Kommunikationssysteme“. Für die an der „Untergruppe Telekommunikation“ des Schengener Exekutivausschusses beteiligten PolizeivertreterInnen war klar, dass diese EU-weite Harmonisierung auf digitalen Standards zu beruhen hatte.

Während analoge Technik Sprache für den Zeitraum der Übermittlung in elektromagnetische Schwingungen übersetzt und zurückübersetzt, funktioniert Digitalfunk ganz anders: Sprache und Daten werden in die bekannten 0 und 1 Bit-Folgen gewandelt und als digitale Päckchen auf die Reise geschickt. Und zwar mit Hilfe einer umfangreichen technischen Infrastruktur. Fortan sind althergebrachte Termini wie senden, empfangen, Kanal etc. ohne Bedeutung.

Über drei in hierarchischer Folge angeordnete Rechner werden die Päckchen, völlig unabhängig davon, ob sie Wörter, Datensätze oder Bilder repräsentieren, fortan nur mehr verwaltet bzw. „gehandelt“.[6] Die Transmission Base Station (TBS) registriert einen gewünschten Verbindungsaufbau und organisiert ihn; das Local Switching Center (LSC) identifiziert die Verbindungspartner, weist beiden eine Funkzelle zu und protokolliert das Ganze; das Mobile Switching Center (MSC) schließlich wacht über die Gesamtheit der eingebuchten Geräte, prüft ihre Identität, ihren Status, ihre Zulassungen und Genehmigungen und registriert das Ein- und Ausbuchen von Funkgeräten. Ferner fungiert es als Gateway, als Schnittstelle in andere Netze: in das öffentliche Telefonnetz, in polizeiliche Datennetze (INPOL) oder in digitale Netze mit divergierenden Standards. Im Millisekundenbereich laufen in diesen Großrechnern hochkomplexe Prozesse ab. Eine personalbesetzte Leitstelle ist überflüssig. Verschlechterte in den „guten alten“ Sprechfunkzeiten ein kleines mechanisches Malheur lediglich die Verständlichkeit des Funkpartners, so legt jedes Hard- oder Softwareproblem bei der neuen Funkgeneration die Verbindung insgesamt lahm: Alles oder Nichts! „Dann reicht’s noch nicht

6 Linde, C.: BOS-Funk, Poing 2002

mal zum Hilfe schreien“, wie ein uns bekannter Leitstellenfunker aus Schleswig-Holstein kritisch anmerkt.

Dass die Zukunft nur digital sein konnte, stand für die Sicherheits- und Ordnungs-Spezialisten von Anfang an fest. Für 500.000 Teilnehmer der BOS musste ein Funknetz her. Ab 1992 legte man im Rahmen von Schengen die Standards fest und einigte sich mit der Nato auf die Übernahme des Frequenzbereichs 380-400 MHz, der für das Militärbündnis nach dem Ende der Ost-West-Konfrontation überflüssig geworden war. Die Untergruppe TK formulierte auch die betrieblichen Anforderungen.

Auf bundesdeutscher Ebene sekundierte die Innenministerkonferenz (IMK) 1994 die europäischen Überlegungen. In der Fortschreibung des Programms „Innere Sicherheit der Bundesrepublik Deutschland“ forderte sie „aufgrund der erkannten gegenwärtigen Mängel“ einen europäischen Sprech- und Datenfunk auf digitaler Basis. Die Formulierung erweiterte en passant die ursprüngliche Vorgabe des Art. 44 SDÜ, der den grenznahen Bereich behandelt, und machte die bundesweite Digitalisierung des Funkverkehrs zum Programm.

Dass der Aufbau digitaler Funknetze nicht nur eine allgemeine Modernisierung bringt, sondern den Polizeien auch einen enormen Zuwachs an Kontrolle beschert, taucht in der ganzen Debatte nicht auf. Dieser Zuwachs bezieht sich einerseits auf die Kontrolle über die BürgerInnen: JedeR PolizistIn hätte mit dem neuen Gerät vor Ort und blitzschnell unmittelbaren Zugriff auf die polizeilichen Datenbanken. Die Überprüfung von Personen, Fahrzeugen und Sachen beschleunigt sich um den Faktor zehn.[7]

In den Blick rücken andererseits die „Vollzugskräfte“ selbst: Mit der Einführung der digitalen Technik bekäme die individuelle Kontrolle des Polizeipersonals eine neue Qualität, und es verwundert, dass gerade die Gewerkschaft der Polizei (GdP) zu den energischsten BefürworterInnen der neuen Funkgeneration gehört. Jedes einzelne Funkgerät ist nur mit einem persönlichen Kennzeichen (PIN) in Betrieb zu nehmen, jeder Funkspruch, jede Anfrage ist individuell und dauerhaft zuzuordnen – ein Maß an Kontrolle, das eineR PolizistIn rasch zum Nachteil gereichen kann: „Nicht gehört“ oder „falsch verstanden“ wird als Rechtfertigung oder Ausrede zukünftig nicht mehr gelten.

---

7 Hesselmann, N.: Digitale Signalverarbeitung, Würzburg 1987

Europäische Funkverwirrung

Die Probleme kamen jedoch weder von den BürgerInnen noch von der polizeilichen Basis. Vielmehr stellte sich schon Mitte der 90er Jahre heraus, dass der Traum eines europaweit einheitlichen Digitalfunk-Standards vorerst nicht zu realisieren war. Im Schengener Rahmen hatte man ab 1992 Anforderungskataloge für den Digitalfunk erstellt. Das European Telecommunications Standards Institute (ETSI) begann wenig später mit der Erarbeitung eines Standards mit dem Namen TETRA. Das Kürzel stand anfangs für Trans European Trunked RAdio und wurde, so Horst Beckebanze vom Polizeitechnischen Institut der Polizei-Führungsakademie, „im Hinblick auf den später anvisierten Weltmarkt" in TErrestrial Trunked RAdio umbenannt. „Während ETSI den Standard TETRA erst noch erarbeitet, befindet sich seit 1993 ein anderes für den professionellen Betriebsfunk konzipiertes digitales Bündelfunksystem bereits auf dem Markt. Es handelt sich dabei um eine vom französischen Staat geförderte Entwicklung der Firma Matra Communication."[8] Dessen Name: Tetrapol.

Allerdings, so Beckebanze, sind „Geräte nach den beiden genannten Standards ... grundsätzlich nicht kompatibel. Man muss sich also für ein System entscheiden." 1996 tat Frankreich dies im Alleingang und führte bei der Gendarmerie und der Police Nationale – wen wundert's – das System der französischen Firma Matra ein. Mit dieser Festlegung eines maßgeblichen Schengen-Staates war die erhoffte europäische Einheitlichkeit vorbei.[9] Die zukünftigen EU-Mitglieder Tschechien und Slowakei sowie die kurz vor der Schengen-Integration stehende Schweiz optierten wie die spanische Guardia Civil ebenfalls für Tetrapol. Belgien, die Niederlande, Dänemark, Österreich, Großbritannien, Irland sowie einige der autonomen Polizeien des spanischen Staates entschieden sich dagegen für den TETRA-Standard.

1999 wurde die Schengen-Kooperation in den Rahmen der EU integriert. Seitdem bemüht sich die Polizeiarbeitsgruppe des Rates der Innen- und Justizminister um eine Schadensbegrenzung. Gemeinsam mit der Industrie und dem ETSI sucht man nach Lösungen, die bei grenzna-

8 Beckebanze, H.: Sichere und gesicherte Kommunikation auch über Grenzen hinweg, in: Polizei – heute 2003, H. 3, S. 68-71 (70)

9 Saupp, H. Sachstand der Einführung des Digitalfunks, in: Magazin für die Polizei 2002, H. 313, S. 4-6 (6)

hen oder gemeinsamen Polizeieinsätzen doch noch eine begrenzte Kommunikation zwischen Geräten der verschiedenen Standards ermöglichen könnten.[10]

Das liebe Geld

Auch im innerdeutschen Rahmen lief die Sache nicht so rund, wie sich Innenministerien und Polizeiführungen erhofft hatten. Im ersten Halbjahr 1998 starteten Berlin und Brandenburg mit mehreren Herstellerfirmen einen Klein-Versuch mit sehr wenigen Geräten auf der Basis des TETRA-Standards. Als dessen Ergebnis hielt die 1996 von den zuständigen Arbeitskreisen der IMK eingesetzte „Projektgruppe Digitalfunk" die „grundsätzliche Funktionsfähigkeit" des TETRA-Standards sowie „generelle Tauglichkeit für BOS-Zwecke und gute Sprachqualität" fest.

Ein Großversuch im Raum Aachen für 1999/2000 sollte weitere Klarheit bringen. Dieses Pilotprojekt startete wegen einer Ausschreibungspanne allerdings erst Mitte 2001. 2.000 BOS-Angehörige wurden mit 135 Stationen, 250 Fahrzeuggeräten, 550 Handgeräten und 20 Meldeempfängern versorgt. In das System eingeschlossen ist auch die „Inhouse-Versorgung" des Großklinikums Aachen. Das Testgebiet maß 715 qkm. In einer zweiten Stufe von Dezember 2001 bis Dezember 2002 wurde die grenzüberschreitende Kommunikation mit den belgischen und niederländischen Behörden getestet.[11]

Der Pilotversuch war Teil des im November 2000 von der IMK genehmigten Zeitplans für die Einführung des Digitalfunks. Die Organisation des Projekts übertrugen die Minister einer eigens gegründeten „Zentralstelle für die Vorbereitung der Einführung Digitalfunk" (ZED), die über ein „Interessenbekundungsverfahren" geeignete Anbieterfirmen und Betreibermodelle ermitteln und Vorschläge für eine Kostenverteilung zwischen Bund und Ländern erarbeiten sollte. „Spätestens" im Mai 2001 wollte man die Finanzierung geklärt haben. Der Januar 2002 war als „spätester Zeitpunkt für den Beginn des Netzaufbaus" vorgesehen. Im Dezember 2005 sollten alle staatlichen BOS angeschlossen sein.[12]

---

10 Projektgruppe Digitalfunk (Saupp, H.): Interworking zwischen TETRA und Tetrapol, www.pilotprojekt-digitalfunk-aachen.de/seite11.htm

11 Saupp, H.: Fahrplan des BOS-Digitalfunks, in: Magazin für die Polizei 2001, H. 300, S. 9-11 (9)

12 ebd., S. 11

Der Zeitplan ist inzwischen Makulatur. Ausschlaggebend dafür waren vor allem die zu erwartenden Kosten für die bundesweite Einführung des Digitalfunks, die im Laufe des Jahres 2001 erstmals ernsthaft diskutiert wurden. Zwar waren auch zu früheren Zeitpunkten schon Zahlen genannt worden. So sprach BGS-Oberrat Erwin Schmalkoke im Juni 1999 auf einem vom Bundesinnenministerium veranstalteten Seminar zur „grenzüberschreitenden polizeilichen Zusammenarbeit zwischen den Schengen-Staaten“ über Aufwendungen von 100 Mio. Euro für die Infrastruktur plus fünf Mio. Euro jährliche Betriebskosten.[13] Die Zahlen bezogen sich jedoch dem Thema des Seminars gemäß nur auf den grenznahen Bereich.

Mit dem Interessenbekundungsverfahren kamen hingegen Schätzungen für das Gesamtprojekt auf den Tisch. Diese bewegten sich zunächst zwischen fünf und 7,5 Mrd. Euro.[14] GdP-Chef Konrad Freiberg hielt den damaligen Maximalbetrag im Juli 2001 für problemlos – „gut investiert in den Einstieg ins digitale Zeitalter“.[15] Für die ZED schien selbst im Jahr darauf Geld noch überhaupt keine Rolle zu spielen. „Bezüglich der Finanzierung“, so BKA-Funkspezialist Herbert Saupp, „vertritt die ZED die Auffassung, dass sich das Projekt nicht nach der (wie auch immer festgestellten) Verfügbarkeit von Mitteln richten kann, sondern der Aufbau eines modernen, den aktuellen Anforderungen der BOS entsprechenden Kommunikationssystems im Vordergrund stehen muss.“[16] Im Spätsommer 2002 sprach Bundesinnenminister Otto Schily wiederum von 7,5 Mrd. Euro, meinte allerdings lediglich die Ausgaben für die Netzinfrastruktur, mit denen noch kein einziges Funkgerät gekauft ist, das dieses Netz auch nutzen könnte.[17] Faktisch hieß das, dass mit Gesamtkosten von neun bis zehn Mrd. Euro zu rechnen war.

Ab Mitte 2002 war klar, dass die Innenminister ihre Rechnung buchstäblich ohne den Wirt gemacht hatten. Bereits im Juni hatte die Finanzministerkonferenz (FMK) verdeutlicht, dass der genannte Betrag nicht realistisch sei. Da die Innenminister auf den Digitalfunk nicht verzichten wollten, setzten sie im selben Monat eine „Gruppe Anforderungen

13 Schmalkoke, E.: Grenzüberschreitende Kommunikationssysteme, in: Grenzüberschreitende polizeiliche Zusammenarbeit zwischen den Schengen Staaten, Seminar v. 13.–16.6.1999, Berlin, Erfurt 2000, S. 158-175 (168)

14 Der Spiegel 48/2002, S. 44f.

15 Gewerkschaft der Polizei, Bundesvorstand: Pressemitteilung v. 13.7.2001

16 Saupp a.a.O.(Fn. 9), S. 5

17 Digitalfunk-Entscheidung ist dringlich, in: Deutsche Polizei 2002, H. 8, S. 3

an das Netz“ ein, die das Projekt auf Mindeststandards abspecken sollte. Die von ihr vorgeschlagene Reduzierung der Funknetzdichte bedeute allerdings, so Beckebanze, „dass in ländlichen Gebieten nur die Funkversorgung für Fahrzeugfunkgeräte sichergestellt wird und in Städten auf eine Versorgung innerhalb von Gebäuden verzichtet werden muss.“[18] Die Kosten blieben trotzdem bei rund 4,5 Mrd. Euro. Nachdem die Finanzminister im November auch diese Version als nicht finanzierbar ablehnten, wurde das Projekt auf der IMK-Tagung vom 5./6. Dezember vorerst gestoppt. Eine gemeinsame IMK/FMK-„Arbeitsgruppe BOS-Digitalfunk“ (AG-BDF) sollte nun retten, was zu retten war.

Das „Geleitzug“-Prinzip, d.h. die zeitgleiche Einführung eines neuen Funksystems im Bund und allen Ländern, wurde aufgegeben, zumal die wenigsten Länder bis zu diesem Zeitpunkt Haushaltsrückstellungen vorgenommen hatten. Die neue von der Ministerpräsidentenkonferenz im Juni 2003 beschlossene Planung sah eine Einteilung in Startländer, die gemeinsam mit dem Bund zwischen 2004 und 2006 ein digitales Funksystem einführen wollten, und Folgeländer vor, die bis 2010 auf den Zug aufspringen sollten.[19] Auch diese Perspektive ist mittlerweile passé, so war aus dem bayerischen Innenministerium zu erfahren. Wenn die Ministerpräsidenten auf ihrer Tagung am 18. Dezember 2003 überhaupt eine „Dachvereinbarung“ beschließen, dann enthält sie wohl sinngemäß folgenden Reim: Jeder fängt mit Digitalfunk an, wenn er es sich leisten kann.

Stephan Stolle ist Redaktionsmitglied von Bürgerrechte & Polizei/CILIP.

18 Beckebanze a.a.O. (Fn. 8), S. 71

19 Bundeseinheitlicher Digitalfunk in weiter Ferne, in: Deutsche Polizei 2003, H. 10, S. 23-25

DNA-Identifizierung

Transformationen einer kriminalistischen Wunderwaffe

von Detlef Nogala

Die forensische DNA-Analytik, irreführenderweise auch als ‚genetischer Fingerabdruck' bezeichnet, hat in der polizeilichen Praxis einen Status erreicht, der politische Initiativen für eine umfassendere Anwendung zur Folge hat. Strittig ist dabei, ob es sich lediglich um ein profanes polizeiliches Identifizierungsinstrument oder doch um einen risikoreichen Eingriff in Grundrechte handelt.

Auch mehr als 20 Jahre nach ihrer Erfindung und im Laufe ihrer weitgehend schon in Routine übergegangenen Anwendung in der kriminalistischen Alltagspraxis hat die forensische DNA-Analyse von ihrer wissenschaftlichen Faszination, aber auch von ihrem Potential für kriminalpolitische und bürgerrechtliche Kontroversen nur wenig eingebüßt. Weitgehend geklärt ist mittlerweile, dass sie ein zuverlässiges und effektives Verfahren der Identifizierung von Personen und der Zuordnung von Spurenmaterial hergibt. Hingegen wird erst durch die sich häufenden Hinweise in den Medien auf den Einsatz von DNA-Tests (etwa bei spektakulären Fällen oder prominenten Protagonisten) sowie die jüngsten Gesetzesinitiativen zur Ausweitung forensischer DNA-Datenbanken deutlicher, welche Möglichkeiten diese Technologie birgt und welche Rolle sie im gesellschaftlichen Zusammenleben in Zukunft spielen wird. Vieles deutet darauf hin, dass die forensische DNA-Analytik eine neue Entwicklungsstufe erreicht hat und dabei ist, ihr Überführungs- wie ihr Überwachungspotential weiter zu entfalten. Allerdings überdeckt die „Normalisierung" des polizeilichen Gebrauchs nur oberflächlich die kritischen Fragen und Bedenken, die von Beginn an mit dem Einsatz dieses Mittels verknüpft waren und angesichts der technischen Weiterentwicklung anhalten. Dazu gehören neben juristisch-politischen auch kriminalethische und kriminalökonomische Einschätzungen und Positionen. In diesem

Zusammenhang kann angesichts einer langen und sich fortsetzenden internationalen kontroversen Diskussion den gegenwärtig zu beobachtenden Ansätzen, einen ‚genetischen' als simples Äquivalent zum händischen Fingerabdruck darzustellen, nur ein untauglicher Versuch zur Reduktion von Komplexität attestiert werden.

Grundlagen und gegenwärtiger Stand der Technik

Das gegenwärtige System der DNA-Identifizierung und die gesamte Debatte darum fußt im Kern auf drei grundlegenden, uns gegenwärtig bekannten Sachverhalten:

Im Konstruktionsplan unserer körperlichen Existenz scheint – erstens – mit dem Aufbau unserer DNA ein Individualisierungsmerkmal vorzuliegen, das uns trotz der Tatsache, dass wir über 99 % der Gene mit unseren Mitmenschen teilen, von allen anderen ziemlich eindeutig unterscheidbar macht. Es sind – nach Stand geltender Erkenntnis – allein schon die sich in großer Zahl wiederholenden so genannten nicht-codierenden Abschnitte unserer DNA-Stränge, die so überaus variabel sind und sich damit „individualisierend" auswirken. Nicht-codierend bedeutet hier, dass sie nicht funktioneller Bestandteil der eigentlichen Gene sind, die der Entwicklung unserer körperlichen Anlagen und unseres Phänotyps, also der äußeren Erscheinungsform, zugrunde liegen. Wir sind also, bei allen Gemeinsamkeiten, im Prinzip nicht nur sozial, sondern auch genetisch gesehen „markierte Individuen".

Der Mensch ist – zweitens – eine hochgradig stoffwechselnde Spezies. In dieser Eigenschaft hinterlässt er bei einer Reihe basaler Lebensvorgänge permanent und ohne es vollständig kontrollieren oder vermeiden zu können, kleine bis kleinste Mengen an DNA-haltigem Zellmaterial. Beim Niesen, Husten, Sprechen verteilt er seine Zellen ebenso sehr in der Umgebung wie durch einfaches Schwitzen, Haarausfall oder bloßes Anfassen von Gegenständen – von reproduktiven Vorgängen ganz zu schweigen. Es ist offenbar so, als hätte die Evolution einer kriminalistischen Laune gefrönt und Vorsorge getroffen: Der Mensch ist ein pausenloser unwillkürlicher Spurenleger.

Zum dritten hat die Biotechnologie mit der DNA-Analyse ein Verfahren entdeckt und bereitgestellt, dass erstens in der Lage ist, mit hoher prinzipieller Zuverlässigkeit die Übereinstimmung von zwei DNA-Proben nachzuweisen, zweitens dies inzwischen für geringste Mengen bis hinunter auf eine einzige Zelle zustande bringt und drittens eine standardi-

sierte Übersetzung von biostofflichen Eigenschaften in computerkompatible und damit datenbankfähige Zahlenformate leistet.

Auch wenn man sich vergegenwärtigt, dass in die Entwicklung der biotechnischen Industrie viel profittrachtendes Kapital gesteckt wurde, ist es beachtlich, welche technischen Fortschritte bei der DNA-Analytik in relativ begrenzten Zeiträumen erreicht worden sind. Noch bis Mitte/Ende der 80er Jahre waren die Kriminaltechniker bei der Auswertung biologischer Tatortspuren auf die im Vergleich gröberen und mit niedrigpegeligen Wahrscheinlichkeiten operierende forensische Serologie verwiesen, bis sich relativ schnell die von Alec Jeffreys und seinen Mitarbeitern in England entwickelte ursprüngliche Variante der DNA-Analyse nach dem RFLP-Verfahren in den kriminaltechnischen Labors verbreitete. Bei dieser Methode waren allerdings relativ große Mengen an analysierbarem DNA-Material erforderlich und der Prozess selbst war – wenn auch sehr zuverlässig – langwierig und kostspielig. Es dauerte allerdings nicht lange, bis mit dem PCR-Verfahren eine weiterentwickelte Methode folgte, die sich ab Mitte der 90er Jahre allgemein als Standard durchsetzte und vor allem den Vorteil bot, mit weit geringeren Mengen an Ausgangsmaterial auszukommen. Hierbei werden einzelne DNA-Fragmente im Reagenzglas in beliebigen Mengen vervielfältigt – schon eine einzige intakte Zelle reicht im Extremfall aus. Erkauft wird die Verfeinerung des Verfahrens allerdings durch ein erhöhtes Risiko, dass fremde DNA die Probe „verunreinigt“ und fehlerhafte Resultate produziert. In jüngerer Zeit ist noch die Analyse so genannter mitochondrialer DNA möglich geworden, die sich als Fragment auch außerhalb des eigentlichen Zellkerns finden lässt und ein Derivat darstellt. Zwar ist die eindeutige Zuordnung hier sehr stark eingeschränkt, dafür bieten nun auch ausgefallene („telogene“, ohne Zellkern) Haare oder Knochenreste eine gewisse Basis für ein verwertbares DNA-Profil. Das Verfahren ist immer sensitiver und damit die benötigte Menge an Spuren-DNA immer kleiner geworden. Inzwischen reichen durch Hautabrieb bei Kontakt mit Gegenständen bzw. Oberflächen (Griffe, Tastaturen etc.) hinterlassene Zellpartikel, um in bestimmten Fällen verwertbare DNA-Profile zu erzeugen. Paradoxerweise ergibt sich damit für die Kriminaltechniker ein neues Problem: Nicht mehr die ausreichende Menge stellt eine Hürde dar, sondern die durch Fremdkontamination höchst anfällige Sensitivität der Erfassung von DNA: Da wir ständig Zellpartikel überall in unserer Lebenswelt verteilen, wächst die Wahrscheinlichkeit, dass wir aus purem Zufall DNA an einem späteren Tatort hinterlassen und uns als „Falsch-

Positive“ u.U. ungerechtfertigter Verdächtigungen erwehren müssen. Diese Hypersensitivität der Erfassungsinstrumente wirkt sich auf die (oft fallentscheidende) Arbeit der polizeilichen Spurensicherungsdienste ambivalent aus: Der erhöhten Fundwahrscheinlichkeit steht eine gleichermaßen gesteigerte Kontaminationsgefahr gegenüber – was den Prozess bei notwendig hohen Qualitätsansprüchen insgesamt wieder aufwands-, zeit- und kostenintensiver macht.[1]

Die eigentlichen DNA-Analysen der Spur- und Personenproben stellen heute vom Ablauf her kein eigentliches Problem mehr dar und werden heutzutage – in den großen Labors oft schon teilautomatisiert – in Mengen routinemäßig durchgeführt. Mit den Jahren hat sich eine eigene Kleinindustrie der DNA-Analytik entwickelt, die durchaus auch ein gewisses kommerzielles Eigeninteresse an der allgemeinen Akzeptanz und weiteren Verbreitung des von ihr angebotenen forensischen Instrumentariums hat. Immerhin wird heute nach internationalen Maßstäben jede personenbezogene DNA-Analyse mit 50-100 Euro kalkuliert; die Auswertung von bestimmten Tatortspuren dagegen wird mit dem bis zu 20-fachen dieser Kosten veranschlagt.

Der nächste verfahrenstechnische Sprung zeichnet sich schon seit einiger Zeit mit der (von der Firma Nanogen schon lange angekündigten, bisher aber nicht realisierten) Marktreife von handlich tragbaren Geräten ab, in denen so genannte „DNA-Chips“ das gesamte Analyseverfahren miniaturisiert abbilden und in nur noch 20 Minuten ein verwertbares DNA-Profil liefern können. Wenn es soweit ist, würden sich die Ermittler im Feld weitgehend von den Kriminaltechnikern in den Laboren unabhängig machen, und über kurz oder lang könnte jeder Laie im Prinzip von beliebigen Ausgangsproben ein DNA-Profil herstellen. Eine solche Demokratisierung hochsensibler Identifizierungstechniken hätte, als hypermoderne „Wahrheitstechnik“ auch im privaten Bereich eingesetzt, gewiss eine Reihe unerwünschter Nebenfolgen.

Jenseits der Verfahrenstechnik liegt die gegenwärtige Entwicklung aber im diffizilen Übergangsbereich von nicht-codierenden zu codierenden Teilen der DNA bei Tatortspuren; dort also, wo das Ziel der kriminalistischen Anstrengungen die Ermittlung des oder der Spurenleger(s) ist. Heikel ist das vor allem deshalb, weil die Akzeptanz der forensischen DNA-Technik nicht nur in Deutschland bislang auf der strikten Be-

1 DNA-Analyse von Hautabriebspuren, in: Kriminalistik 2003, H. 8-9, S. 497-499

schränkung auf die nicht-codierenden Teile der DNA beruhte. Alle beteiligten Praktiker und Politiker – zumindest in Deutschland – haben diese Beschränkung immer wieder betont und beschworen. Mittlerweile ist jedoch klar, dass bei der DNA-Analyse – contra legem – regelmäßig das Geschlecht der unbekannten Person bestimmbar ist. Ferner lassen sich technisch inzwischen Aussagen über den wahrscheinlichen Phänotyp hinsichtlich Augen-, Haar- und Hautfarbe aus einer DNA-Probe ableiten, die den Kern eines machbaren genetischen Fahndungsbilds darstellen. Der englische Forensic Science Service bietet eine solche Option schon offiziell an; die Niederlande und die Schweiz haben in ihren jüngst erlassenen Gesetzen diese Möglichkeit ausdrücklich normiert.[2] Die absehbaren Fortschritte in diese Richtung, werden in naher Zukunft ohne Zweifel einen Druck auf die bisher vorherrschenden restriktiven Regelungen ausüben und damit eine neue Ära des fahndungspraktisch erweiterten „genetischen Fingerabdrucks“ einläuten.

Das kriminalistisch-kriminalpolitische Kalkül mit der DNA

Die Auseinandersetzung über Funktionalität und Legitimität der DNA-Analyse ist über viele Jahre hinweg mit inzwischen oftmals standardisierten Argumenten geführt worden und dauert an. Idealtypisch lassen sich zwei Lager ausmachen: Dem vornehmlich aus Kriminalisten, Polizeistrategen, Forensikern, Industrielobbyisten und nicht zuletzt (politisch meist konservativ orientierten) Kriminalpolitikern gebildeten Lager der „DNA-Euphoriker“ steht eine Gruppe der „DNA-Skeptiker“ gegenüber, die sich in erster Linie aus praktizierenden wie akademischen Juristen, Datenschutzbeauftragten sowie Bürgerrechtsaktivisten rekrutiert. Während die Ersteren keine wirklichen Gefahren in den Potentialen der für reine Identifikationszwecke eingesetzten DNA-Analyse erblicken können und deshalb vehement für eine Ausschöpfung aller in der Technologie liegenden Möglichkeiten eintreten, werden die anderen nicht müde, die bürgerrechtlichen Risiken durch Missbrauchsoptionen zu betonen und beharren folgerichtig auf einer möglichst beschränkten und justiziell kontrollierten Einsatzpraxis. Die anfangs vernehmbaren Stimmen hingegen, die die kriminalistische Effektivität und forensische Brauchbarkeit der DNA-Analytik grundsätzlich in Zweifel zogen, sind heute weitgehend

2 Benecke, M.: Coding or non-coding, in EMBO reports 2002, no. 6, pp. 498-501

verstummt. Vielmehr ist die Funktionalität der DNA-Analytik als „Mittel der Verbrechensbekämpfung“ zumindest im Bereich der Kapital- und schweren Sexualdelikte von allen Teilnehmern der Debatte weitgehend anerkannt.

Einen wesentlichen Anteil daran hatten fraglos die immer wieder in der Presse publizierten Meldungen über dank einer DNA-Analyse aufgeklärte Kapitaldelikte; einige davon lange Zeit brachliegende Altfälle. Hierin liegt ein wesentliches Element, warum dem „genetischen Fingerabdruck“ der Ruf einer kriminalistischen Wunderwaffe vorauseilt. Was in langen und mühseligen konventionellen polizeilichen Ermittlungen offenbar nicht gelingen wollte, erscheint mit Hilfe des DNA-Vergleichs ein scheinbar spielerisches Unterfangen: die Identifizierung und Überführung der gesuchten Täter. Unter der Maxime, dass Fallaufklärung das oberste Ziel kriminalistischen Wirkens ist – und das bedeutet vor allem die erfolgreiche und gerichtsfeste Zuordnung von Tatortspuren zu identifizierten Tätern – hat die Forderung des Bundes Deutscher Kriminalbeamter (BDK) nach möglichst weitgehendem Ausbau der DNA-Analyse als Ermittlungsinstrument durchaus etwas für sich.[3] Mehr noch: der genetische Fingerabdruck erfüllt in idealtypischer Weise die Erwartungen, die Ex-BKA-Präsident Horst Herold in seinen vorausschauenden Einlassungen den „objektiven Sachbeweisen“ als zentralen Elementen einer modernen Polizeiorganisation zugedacht hatte.

Der tatkräftigen Verkündigung einer kriminalistischen DNA-Erfolgsgeschichte, vor allem in Verbindung mit forensischen DNA-Datenbanken, können sich denn auch die Kriminalpolitiker nicht entziehen. So lobt Bundesinnenminister Schily in einer Fünf-Jahresbilanz die zählbaren Erfolge der beim BKA geführten DNA-Analysedatei[4] und macht sich bei dieser Gelegenheit zum Advokaten für eine Erweiterung des darin erfassten Personenkreises sowie für eine Absenkung der Erfassungsschwelle. Dahinter will die konservative Opposition nicht zurückstehen und bringt ihrerseits als vermeintliche Stimme der kriminalistischen

3 BDK: „DNA-Gesetzgebung: Problemaufriss und Lösungsansätze aus kriminalpraktischer Sicht“ vom 24. Januar 2003; www.bdk-brandenburg.de/fa_030124.html

4 Bundesinnenministerium: Pressemitteilung v. 7.4.2003; laut BKA-Pressestelle verzeichnete die DNA-Datenbank zum 30.9.2003 insgesamt 306.908 Datensätze, davon ca. 86 % personenbezogene Einträge. Seit Einrichtung der Datei wurden 10.766 Zuordnungen von Personen zu Tatortspuren getroffen. In 4.394 Fällen gab es Verbindungen von Tatortspuren. Ca. 87 % dieser Zuordnungen betreffen Diebstahlsdelikte.

Basis ganz aktuell einen Antrag ins Parlament, der im Wesentlichen die Abnahme einer DNA-Probe schon bei der erkennungsdienstlichen Behandlung, den Einbezug so genannter „Einstiegskriminalität“ (Drogen) in die Erfassung sowie die Abschaffung des Richtervorbehalts bei der Untersuchung von anonymen Spurenmaterial aufheben will.[5]

Bei den Innenministerien des Bundes und der Länder scheint sich nun eine Position herauszuschälen, die der DNA-Analytik qua erweiterter Erfassung und Speicherung in der DNA-Datenbank des BKA im Gegensatz zur ursprünglichen Aufklärungs- nun eine deutlich gewichtigere Abschreckungs- und Präventionsfunktion zuschreibt. Der dazugehörige kriminalistische Glaubenssatz lautet: Je größer die Zahl der Datensätze in der Datenbank, desto größer die Zahl der Treffer und damit die der Aufklärungserfolge. Um aber die erfasste DNA-gemusterte Population zu erweitern, wird mit isolierten kriminologischen Erkenntnissen operiert, nach denen Sexualdelinquenten auch durch eine ganze Anzahl, teilweise weniger gravierender Straftaten in Erscheinung treten. Daher müsse konsequenterweise die Erfassungsschwelle niedriger angesetzt werden, um die Gruppe der Sexualstraftäter möglichst vollständig in der Datenbank zu registrieren, was der Ermittlung entsprechender Delikte zugute käme. Je mehr polizeiliche Aufklärung aber, so das Kalkül, umso stärker der Abschreckungs- und Disziplinierungseffekt auf potentielle und rückfällige Straftäter: nur so sei Kriminalität einzudämmen! In der Konsequenz bedeutet dies, dass sehr viel mehr Delinquenten auch für leichtere Delikte mit ihrem Identifizierungsmuster erfasst und ‚überwacht‘ werden.

Die Skeptiker sind in der Defensive und beschränken sich auf die Verteidigung des rechtlichen Status quo. Ihre Beschwörungen abstrakter Gefahren einer möglicherweise künftig drohenden genetischen Ausforschung samt der damit verbundenen Aussonderungsmechanismen verhallen ungehört angesichts der prätentiösen Versprechen der DNA-Datenbank-Apologeten, die Gesellschaft von der Plage der Kindermörder und Rückfalltäter befreien zu können. Dass diese Zusage sich als bloß zweckoptimistisch herausstellen könnte und zu einer an freiheitlich-rechtsstaatlichen Grundsätzen orientierten Kriminalpolitik nicht so richtig passen will, geht im verallgemeinerten rhetorischen Verbrechensbekämpfungsgetümmel schlicht unter.

---

5 Gesetzesantrag der CDU/CSU Fraktion, BT-Drs. 15/2169 v. 9.12.2003

Von der Wunder- zur Allzweckwaffe

Die Extensivierung der forensischen DNA-Erfassung ist nicht bloß ein deutscher, sondern ein – wenn auch nicht einheitlicher – international zu verzeichnender Trend. Weltweit sind 40 nationale Datenbanken in Betrieb, die Hälfte davon in europäischen Ländern.[6] Großbritannien zeigt sich in diesem Fall – wie auch bei der Videoüberwachung – als Vorreiter in der extensiven Nutzung technisch basierter Potentiale für polizeiliche Zwecke. Auch der polizeiliche Kooperations- und Vernetzungsgedanke ist berücksichtigt: Gut eingespielte Netzwerke von Kriminalisten und DNA-Advokaten haben dafür gesorgt, dass in Europa ein einheitliches Verfahren Anwendung findet und somit DNA-Datensätze gegenseitig austauschbar werden. Die gegenwärtige deutsche kriminalpolitische Diskussion um die Aufweichung bzw. Abschaffung der rechtlichen Restriktionen, die einem Ausbau der DNA-Datenbank entgegenstehen, ist in diesem internationalen Kontext zu interpretieren.

Deutlich zeichnet sich ein Trend ab, der die DNA-Analytik, nicht zuletzt durch die Verknüpfung über Datenbanken, von einem umstrittenen, für Ausnahmezwecke gedachten Instrument zur Klärung besonders schwerer Verbrechen, zu einem routinemäßigen, auf die kriminalistische Bearbeitung auch von mittlerer Kriminalität und Massendelikten zielenden Verfahren wandelt. Statt sich auf die Erfassung der extremen und gefährlichen Verbrecher zu beschränken, regen insbesondere die DNA-Datenbanken offensichtlich dazu an, sie als Mittel zur Kontrolle ganzer ‚aktiver krimineller Populationen' einzusetzen. Im Amerikanischen ist ‚function creep' der treffende und schwer zu übersetzende Ausdruck dafür. Die Bundesrepublik befindet sich gegenwärtig offenbar in einem Zwischenstadium, an deren funktionslogischem Ende im negativen Extremfall auch die DNA-Erfassung der gesamten Bevölkerung stehen kann. Immerhin wäre die tatsächliche Abschreckungswirkung der DNA-Verdatenbankung dann empirisch überprüfbar und auch die lästigen und teuren Massengentests blieben den Bürgern auf diese Weise erspart.

Detlef Nogala ist wissenschaftlicher Referent am Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg.

6 Interpol DNA Unit: „Global DNA Database Inquiry 2002", Interpol 2003

Der Krieg im Innern

Biometrische Kontrollen nach dem 11. September

von Jonathan P. Aus

Seit den Anschlägen vom 11. September 2001 wird sowohl in den USA als auch in der EU die systematische Erfassung, Speicherung und Weitergabe biometrischer Daten vorangetrieben. Für biometrisch aufgerüstete Reisedokumente und Grenzkontrollen rücken transatlantisch abgestimmte Standards mit weltweitem Modellcharakter in greifbare Nähe.

Der von der US-Regierung unter George W. Bush geführte „Krieg gegen den Terror" richtet sich nicht nur gegen äußere Ziele wie Afghanistan oder Irak. Die zur „Heimatsicherheit" aufgestellten Behörden suchen verstärkt auch nach Möglichkeiten zur Bevölkerungskontrolle im Innern. An den Grenzen sollen nun biometrische Technologien zum Einsatz gelangen, welche die zweifelsfreie Ermittlung und Überprüfung der (angeblichen) Identität eines Menschen versprechen.

Nicht nur in den USA sehen die Minister der Inneren Sicherheit, ihre Polizeien und die biometrische Industrie automatisierte Fingerabdruck-, Iris- und Gesichtskontrollen als wichtige Bausteine zur Bekämpfung des internationalen Terrorismus an. Tatsächlich ermöglichen biometrische Verfahren die Kontrolle von Leben (griechisch: *bios*) anhand seiner exakten Messung (*metron*). In Verbindung mit modernen Informationstechnologien entfaltet die Biometrie ihr ganzes Kontrollpotential.[1] Theoretisch können mit dieser Technik einzigartige körperliche Merkmale wie

1 vgl. Woodward, J. et al.: Biometrics – Identity Assurance in the Information Age, Berkeley 2002; Nanavati, S. et al.: Biometrics – Identity Verification in a Networked World, New York 2002; Nolde, V.; Leger, L. (Hg.): Biometrische Verfahren – Körpermerkmale als Passwort, Neuwied 2002; Behrens, M.; Roth, R. (Hg.): Biometrische Identifikation, Wiesbaden 2001

Fingerabdrücke, Iris oder Gesicht in maschinenlesbare digitale Codes verwandelt und von Computern gespeichert, ausgetauscht und verglichen werden. In der Praxis hingegen hinken die auf dem Markt der (grenz-)polizeilichen Identifikation angebotenen biometrischen Systeme noch häufig den an sie gestellten Erwartungen hinterher.[2]

Trotz der technologischen Unreife bzw. Unzuverlässigkeit von Verfahren wie der Gesichtserkennung werden biometrische Kontrollen von der US-Regierung rechtlich gefordert und finanziell milliardenschwer gefördert. Schließlich gehe es um die Bekämpfung potentieller und daher nur im Vorfeld abzuwendender Massenmorde à la Twin Towers. Wer im sicherheitspolitischen Ausnahmezustand auf Bürgerrechte und informationelle Selbstbestimmung poche, habe die Gefahr des internationalen Terrorismus offensichtlich nicht erkannt. In der Praxis seien „preemptive strikes" und der Einsatz modernster Technologien erforderlich. So zumindest die Auffassung des US-amerikanischen Department of Homeland Security (DHS), das die Energie seiner rund 170.000 Bediensteten unlängst auf die Entwicklung des neuen US-Grenzkontrollsystems „U.S. VISIT" (United States Visitor and Immigrant Status Indication Technology) gelenkt hat. Die rechtlichen Grundlagen für U.S. VISIT wurden mit dem unmittelbar nach dem 11. September verabschiedeten „USA Patriot Act" gelegt und mit dem „Enhanced Border Security and Visa Entry Reform Act of 2002" weiter vertieft.[3]

U.S. VISIT wird am 1. Januar 2004 – vorerst an den Luft- und Seegrenzen – in Betrieb gehen. Alle AusländerInnen, die nicht im Besitz eines biometrischen Visums oder Reisepasses sind, werden dann nach Betreten des US-Territoriums einer erkennungsdienstlichen Behandlung (Fingerabdrücke und Gesichtsscan) unterworfen. Die so gewonnenen digitalisierten biometrischen Daten sollen, so hofft zumindest das DHS, nicht nur die (angebliche) Identität der einreisenden Person zweifelsfrei bestätigen („one-to-one check"), sondern zusätzlich, mit Hilfe entsprechender DHS-Datenbankanbindungen, mit den bereits erfassten Daten verurteilter Straftäter und mutmaßlicher Terroristen abgeglichen werden

2 vgl. The Economist Technology Quarterly v. 6.12.2003, pp. 17-21

3 House Resolution (H.R.) 3162 und 3525, www.usa.gov

(„one-to-many check“).[4] Aus Zeitgründen ließ man die gesetzlich vorgeschriebene Datenschutzprüfung des Systems bleiben.[5]
Die „preemptive strikes“ der US-Regierung im Bereich der Inneren Sicherheit schlagen zudem auf die Ausgestaltung der Reisepässe von Angehörigen befreundeter Staaten durch, die bislang in den vergleichsweise seltenen Genuss einer visafreien Einreise in die USA kamen. Dies betrifft Staatsangehörige der 27 bislang privilegierten „visa waiver countries“ (namentlich die EU-Mitgliedstaaten außer Griechenland sowie die Schweiz, Norwegen, Australien usw.). Auch für sie gilt: Spätestens bis zum 26. Oktober 2004 müssen AusländerInnen, die in die USA einzureisen gedenken, in der Lage sein, den US-Einwanderungsbehörden einen biometrischen und maschinenlesbaren Pass vorzulegen – ansonsten müssten auch sie biometrische Visa beantragen.[6] Von US-Seite zur raschen Einführung biometrischer Reisepässe gedrängt, sind eine Reihe von EU-Mitgliedstaaten den amerikanischen Forderungen bereits entgegengekommen – so etwa die Bundesrepublik mit dem im Januar 2002 in Kraft getretenen Terrorismusbekämpfungsgesetz.[7]

Biometrische Kontrollen in der EU: Visa, Pässe, Asyl

Auch die EU stellte die Weichen auf systematische biometrische Kontrolle um. Auf ihrem Gipfeltreffen in Thessaloniki im Juni 2003 segneten die Staats- und Regierungschefs (Europäischer Rat) die Einführung biometrischer Visa und Aufenthaltserlaubnisse von Drittstaatsangehörigen sowie biometrischer Pässe für EU-BürgerInnen ab.[8] Nach Willen des Europäischen Rates sollen auch das künftige Visa-Informationssystem (VIS) und die zweite Generation des Schengener Informationssystems (SIS II) Biometrie-kompatibel gemacht werden.[9]

---

4 Der Tagesspiegel v. 21.5.2003

5 US Senate Committee on Governmental Affairs: Pressemitteilung v. 4.12.2003, http://govt-aff.senate.gov/

6 vgl. Biometric Technology Today: Visa waiver countries set tight deadline by USA, May 2002, p. 2. Siehe auch U.S. General Accounting Office: Border Security: Implications of Eliminating the Visa Waiver Program, Washington 2002, GAO-03-38, www.gao.gov

7 Bundesgesetzblatt Teil I 2002, Nr. 3, S. 361-395, insbes. Art. 7-8 zur Änderung der Pass- und Personalausweisgesetze. Eine zentrale biometrische Referenzdatei dürfte danach für Pässe und Personalausweise von Deutschen nicht eingerichtet werden.

8 European Council: Presidency Conclusions – Thessaloniki, 19-20 June 2003, no. 11

9 European Council: Presidency Conclusions – Brussels, 16-17 October 2003, no. 31

Bei so starkem politischen Rückenwind ließ die Europäische Kommission, die spätestens seit dem Inkrafttreten des Vertrags von Amsterdam im Mai 1999 zu einer Wegbereiterin der EU-Innen- und Justizpolitik geworden ist, nicht lange mit konkreten Vorschlägen auf sich warten. Ende September 2003 präsentierte sie ein erstes Paket von Verordnungsentwürfen zu biometrischen Visa und Aufenthaltstiteln.[10] Der Rat der Innen- und Justizminister hat diese Vorschläge, die auf Forderungen des deutschen Bundesinnenministeriums zurückgehen, noch im November 2003 grundsätzlich begrüßt.[11] Momentan wird in Brüssel an den technischen Details der biometrischen Visa und Aufenthaltstitel sowie an rechtlichen Grundlagen für biometrische Reisepässe von UnionsbürgerInnen gefeilt. Letztere dürfte die Kommission noch vor Jahresende 2003 vorgelegen. Das Europäische Parlament wird, dem parlamentarisch-demokratischen Defizit und exekutiven Überschuss der EU entsprechend, lediglich angehört.

Die Kommission kann bei der Ausarbeitung ihrer neuesten Verordnungsvorhaben auf ihre Erfahrungen als Betreiberin des biometrischen Systems Eurodac zurückgreifen, das seit dem 15. Januar 2003 EU- bzw. Schengen-weit (mit unbedeutenden Sonderregelungen für Norwegen, Island und Dänemark) in Betrieb ist.[12] Eurodac ist ein automatisches Fingerabdruck-Identifizierungssystem (AFIS). Es betrifft die Schwächsten der Schwachen: Asylsuchende und so genannte „Illegale“. Ihnen werden nun bei Einreichung ihres Asylantrags innerhalb des EU-europäischen „Raums der Freiheit, der Sicherheit und des Rechts“ oder nach fehlgeschlagenem Versuch des unbemerkt-irregulären Überschreitens der EU-Außengrenzen alle zehn Finger gescannt. Ihre Fingerabdruckdaten landen im Zentralrechner der Europäischen Kommission, der allen angeschlossenen Einheiten in Sekundenschnelle nach dem Prinzip „hit/no hit“ Auskunft gibt, ob die Person bereits gespeichert ist. Ein Treffer bedeutet, dass sie schon einmal einen Asylantrag gestellt hatte oder beim heimlichen Grenzübertritt angetroffen worden war.

10 KOM (2003) 558 endg.

11 EU-Ratsdok. 14995/03; Bundesinnenministerium: Pressemitteilung v. 27.11.2003

12 vgl. Aus, J.: Supranational Governance and Domestic Change in an “Area of Freedom, Security and Justice”: Eurodac and the Politics of Biometric Control, SEI Working Paper No. 72, Brighton 2003, www.sei.ac.uk; Brouwer, E.: Eurodac: Its Limitations and Temptations, in: European Journal of Migration and Law 2002, Vol. 4, pp. 231-247; Van der Ploeg, I.: The Illegal Body: “Eurodac” and the Politics of Biometric Identification, in: Ethics and Information Technology 1999, Vol. 1, pp. 295-302

Die Wurzeln der Eurodac-Verordnung vom 11.12.2000 liegen im europäischen Binnenmarktprojekt und im Dubliner Asylübereinkommen von 1990, das im Februar 2003 in eine gemeinschaftsrechtliche Verordnung überführt wurde.[13]

Transatlantische Harmonisierung technischer Standards

Ob Fingerabdruck-, Iris- oder Gesichtskontrollen: die zum Krieg gegen den Terror und zur Bekämpfung von illegaler Einwanderung und „Asylmissbrauch" aufgerufenen Sicherheitsapparate üben sich mit Hilfe biometrischer Technologien in präventiver Repression. Damit der Austausch biometrischer Daten nicht an nationalstaatlichen Grenzen stecken bleibt, müssen jedoch multilateral abgestimmte biometrische Verfahren und gemeinsame technische Standards her. Leichter gesagt als getan, erweisen sich doch die zur Auswahl stehenden biometrischen Verfahren als sehr unterschiedlich – was durchschnittliche Fehlerraten und Belastungsgrenzen betrifft, aber auch hinsichtlich Kompatibilität mit polizeilichen Datenbanken, öffentlicher Akzeptanz, Kosten und Patentrechten.[14]

So liegt z.B. die öffentliche Akzeptanz bei dem als herkömmliche Fotografie verkleideten Gesichtsscan erheblich höher als bei der Erfassung von Fingerabdrücken, die den Beigeschmack des Kriminellen nicht los wird. Andererseits ist die Gesichtserkennung bislang noch ein technisch mangelhaftes Verfahren mit inakzeptabel hoher durchschnittlicher Fehlerrate. Ein biometrisches System, das sogenannte „Nutzer" entweder fälschlicherweise zurückweist oder akzeptiert, würde ständig Fehlalarme produzieren und mutmaßliche StraftäterInnen kaum identifizieren können. Selbst wenn sich die Gesichtserkennungstechnik in den nächsten Jahren erheblich verbessern sollte, ist noch nicht abzusehen, ob und wann polizeiliche Träume wie die Kopplung von Biometrie und Videoüberwachung Wirklichkeit werden könnten.

Demgegenüber sind Fingerabdruckverfahren in puncto technische Zuverlässigkeit kaum zu überbieten.[15] AFIS wie Eurodac können zudem

13 Verordnung Nr. 343/2003, in: Amtsblatt der EG Nr. L 50 v. 25.2.2003, S. 1-10

14 vgl. TeleTrust Deutschland e.V.: Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren, Erfurt 2002, www.teletrust.de

15 So gelang es der Firma Bioscript im Jahre 2002 mit 0,19 % die geringste „equal error rate" der jährlich stattfindenden „Fingerprint Verification Competition" zu erzielen; vgl. Biometric Technology Today: FVC 2002 entrants set new high verification standards, October 2002, p. 2.

an Jahrzehnte polizeilich-daktyloskopischer Praxis und bereits existierende polizeiliche Referenzdateien anknüpfen. In einem AFIS werden gewöhnlich die Fingerabdruckdaten unter einer Nummer gespeichert, die den Link zum entsprechenden polizeilichen Personenindex bildet. Gerade für die Kriminalpolizeien ist die Kompatibilität von nationalen AFIS mit supranationalen Systemen wie dem SIRENE-Netzwerk der Schengen-Gruppe von herausragender Bedeutung. Diese polizeiliche Vorliebe wurde auch von der biometrischen Industrie und ihren Dachverbänden wie der International Biometric Industry Association (IBIA) erkannt.[16] Die Steria Gruppe z.B. versorgt nahezu alle Schengen- und EU-Mitgliedstaaten sowie die Schweiz mit sogenannten „Fingerprint Image Transmission"-Geräten, die alle nationalen AFIS mit Eurodac verbinden können.[17] Die Firma Sagem, die u.a. die AFIS von Deutschland, Österreich und Frankreich betreibt, hat unlängst auch den afrikanischen Markt der Bevölkerungskontrolle für sich erschlossen.[18] So mussten z.B. im Vorfeld der mauretanischen Wahlen vom Oktober 2001 alle BürgerInnen dieses hochgradig autoritär regierten Landes ihre Fingerabdrücke in einem biometrischen Zentralrechner hinterlegen, um anschließend mit von Sagem entwickelten „smart cards" versorgt zu werden.[19] Zur Rechtfertigung wurde von Regierungsseite die Verhinderung von Wahlbetrug angeführt – erstaunlich, hatte sich Präsident Taya im Jahre 1984 doch selbst an die Macht geputscht und seinen wichtigsten Gegenkandidaten bei den Präsidentschaftswahlen von 2003 kurzerhand in Haft nehmen lassen.[20]

Bliebe da noch das biometrische Verfahren der Iriserkennung, das etwa von der Firma Johan Enschedé in Rotterdam an Asylsuchenden erprobt wurde. Die gleiche Technologie wurde auch am Flughafen Amsterdam Schipol getestet, um registrierten Geschäftsreisenden und „frequent flyers" lange Wartezeiten beim Check-in zu ersparen.[21] Der ent-

16 www.ibia.org

17 www.steria.no/fit, sowie Steria Group: Pressemitteilung v. 14.1.2003, www.steria.com. Die Fingerabdruckscanner der US-"Citizenship and Immigration Services" werden von der Firma Identix gestellt.

18 vgl. Sagem Group: Sagem – The major player in the Eurodac system, Press Release of January 22, 2003, www.sagem.com

19 vgl. Biometric Technology Today: Voting success in Mauritania, February 2002, p. 1

20 Frankfurter Allgemeine Zeitung v. 10.11.2003

21 Biometric Technology Today: Iris technology gets the green light in Holland, January 2002, p. 4, vgl. zudem www.eyeticket.com

scheidende Haken an der noch blutjungen und vergleichsweise kostspieligen Iriserkennung ist jedoch, dass sich das Patent dieses Verfahrens im Besitz der US-amerikanischen Firma Iridian Technologies Inc. befindet.[22] Die deshalb zu erwartenden hohen Kosten waren für die Europäische Kommission Grund genug, vorerst die Finger von der Iriserkennung zu lassen.[23]

Was das künftige VIS und SIS II sowie biometrische Pässe in der EU anbelangt, wird es daher aller Voraussicht nach zu einer Kombination unterschiedlicher biometrischer Verfahren kommen, namentlich von Fingerabdruck- und Gesichtserkennungstechnik.[24] Schließlich könne zum gegenwärtigen Zeitpunkt nur ein multi-biometrischer Ansatz die Sicherheit von Reisedokumenten garantieren. Wahrscheinlich ist auch der Einsatz von kontaktlosen Mikrochips als Speichermedium für biometrische Informationen in maschinenlesbaren Reisedokumenten.[25]

Eine offizielle politische Entscheidung zur Auswahl der biometrischen Verfahren steht noch aus. Diese trifft die EU nicht alleine. Vielmehr verhandelt man gegenwärtig im Rahmen der International Civil Aviation Organisation (ICAO) und der G8-Gruppe.[26] Einmal festgeklopft dürften sich die von EU und USA abgestimmten Positionen jedoch zu weltweiten Standards entwickeln. Innenminister Otto Schily und Heimatschutzminister Tom Ridge haben sich Ende Oktober in Berlin bereits auf Fingerabdrücke und Gesichtsscans festgelegt.[27]

Jonathan P. Aus ist Research Fellow bei ARENA (Advanced Research on the Europeanisation of the Nation-State), Universität Oslo.

22 www.iridiantech.com. Hinter dem Patent steht die Arbeit von Daugman, J.: High confidence visual recognition of persons by a test of statistical independence, in: IEEE Transactions on Pattern Analysis and Machine Intelligence 1993, No. 11, pp. 1148-1161

23 KOM (2003) 558 endg., S. 5

24 KOM (2003) 323, S. 4

25 KOM (2003) 558 endg., S. 11

26 EU-Ratsdok. 12521/03, 14776/03, 10857/03 u. 12171/03; G8 Justice and Home Affairs Ministerial Meeting – Paris, 5 May 2003: Final Official Statement, www.g8.fr/evian/english/home.html und www.g7.utoronto.ca

27 Financial Times Europe und Financial Times Deutschland v. 31.10.2003

Überwachte Fahrt für freie Bürger?

Automatische Nummernschilderkennung

von Daniel Boos

Die Koppelung von Videokamera und Computer macht es möglich. Automatische Fahrzeugnummern-Erkennungssysteme ermöglichen nicht nur die Erhebung von Straßengebühren, sondern auch polizeiliche Kontrollen.

Seit es sie gibt, sind Autonummern für die Polizei interessant, weil sie nicht nur die Identifikation des Fahrzeugs, sondern auch die seines Besitzers ermöglichen. Sie sind eindeutig und außerdem in einem zentralen Register bzw. einer nationalen Datenbank erfasst. Die Abfrage dieses Registers erfolgte bisher zumeist manuell, d.h. einE PolizistIn musste das Kennzeichen per Funk an eine Zentrale übermitteln oder – im günstigsten Fall – direkt in ein Datenfunkgerät eingeben.

Das große Verkehrsaufkommen und die beschränkten Ressourcen führten jedoch dazu, dass nur ein sehr kleiner Anteil von Fahrzeugen überhaupt überprüft werden kann.[1] Die seit der Mitte der neunziger Jahre entwickelte Technik der automatischen Fahrzeugnummernerkennung soll hier Abhilfe schaffen: Automatische Fahrzeugnummernschild-Erkennungssysteme (AFNES) „lesen“ das von einer Videokamera übertragene Bild der Autonummer und führen – je nach Einsatzzweck – direkt eine Abfrage in einer bestehenden Datenbank durch. Neuere Systeme können dabei bis zu 3.000 Nummern pro Stunde erkennen, selbst wenn die Autos mit einer Geschwindigkeit von 160 km/h passieren.[2] Es handelt sich im Prinzip um eine automatisierte Videoüberwachung, bei der im Gegensatz zur herkömmlichen Videoüberwachung nicht nur die

1 Norris, C.; Armstrong, G.: The Maximum Surveillance Society, Oxford 1999, p. 214
2 www.met.police.uk/job/job905/live_files/4.htm

Bilder übertragen und aufgezeichnet, sondern zugleich auch analysiert werden. Ein Mustererkennungsverfahren wandelt das Bild eines Fahrzeugschildes in Text um, der vom Computer weiter verarbeitet und z.B. abgeglichen werden kann. Neben fix installierten Systemen bietet der Markt mittlerweile portable Geräte oder den Einbau in Autos an. Auch der Anschluss an geschlossene Videoüberwachungssysteme (closed circuit television – CCTV) ist möglich. Die Einsatzgebiete reichen von der Verkehrsüberwachung über die Erhebung von Straßengebühren oder die Überwachung von Zufahrtsberechtigungen bis hin zu polizeilichen oder gar geheimdienstlichen Zwecken.

Die Mischung von verschiedensten Einsatzzwecken war bereits beim ersten Einsatz von Kennzeichenerkennungssystemen sichtbar. In den 70er Jahren waren zu Zwecken der Verkehrsüberwachung Videokameras an den Ringstraßen um die Londoner City installiert worden. Nach Anschlägen der IRA Anfang der 90er Jahre wurden sie an ein AFNES angeschlossen, das die Abfrage polizeilicher Datenbestände ermöglichte. „Your number could be on", titelte die „Times" am 13. Mai 1994. Der „Ring of Steel" ermöglichte es ferner, so Steve Wright von der Omega Foundation, den Weg von Autos um die City herum, ihre Ein- und Ausfahrt aus dem umschlossenen Gebiet nach zu verfolgen.[3]

Vom stählernen Ring ist auch bei dem aktuell bekanntesten Projekt des großflächigen Einsatzes der automatischen Fahrzeugnummernerkennung die Rede: Um das Verkehrsaufkommen in der City zu reduzieren, kassiert die Londoner Stadtregierung seit dem 27. Februar 2003 eine Gebühr für die Fahrt in die Innenstadt. Die Eingangspunkte zu einer Fläche von 21 km^2 werden dazu von 203 fix installierten Kameras überwacht. Das angeschlossene AFNES soll prüfen, ob die FahrzeughalterInnen die Maut bezahlt haben. Die Erkennungsrate liege bei 90 %.[4] Die Stadtregierung will die Fahrzeug-Erkennung beibehalten, auch wenn sich herausstellen sollte, dass die Maut zur Ausdünnung des Verkehrs untauglich sei. Sie soll helfen, die Hauptstadt gegen terroristische Angriffe zu schützen. Laut „Observer" waren der britische Inlandsgeheimdienst MI 5 und die Staatsschutzabteilung der Metropolitan Police (Special

3 Wright, S.: Auf dem Weg zum globalen Überwachungsstaat, in: Bürgerrechte & Polizei/ CILIP 61 (3/1998), S. 43-51 (46)

4 www.tfl.gov.uk/tfl/cc_fact_sheet_key_numbers.shtml

Branch) seit dem 11. September 2001 an der Entwicklung des Systems beteiligt.[5]

Projekt Laser

Großbritannien ist nicht nur Vorreiter bei der Videoüberwachung, sondern auch bei der Nummernschilderkennung. Zur Evaluation und Förderung ihres polizeilichen Einsatzes betreiben die britischen Polizeien ein umfassendes Programm namens „Project Laser – Denying criminals the use of the roads“ (Kriminellen die Benutzung der Straße verweigern).[6] Die bei der Fahrzeugerkennung anfallenden Daten werden dabei über das Police National Network mit dem Versicherungsregister, dem Führerschein- und Fahrzeughalterregister (DVLA), dem Police National Computer (PNC) sowie lokalen polizeilichen Datenbanken abgeglichen.

Mit Unterstützung u.a. des Innenministeriums integrierte etwa die Polizei von Northamptonshire ein AFNES in ein bereits bestehendes geschlossenes Videoüberwachungssystem.[7] Bei einer Evaluation von April bis Dezember 2001 lösten 1,5 % der Autos im Aufnahmebereich der Kameras einen Alarm aus. Da das Einsatzteam nur aus sechs Beamten bestand, habe man nur auf 8 % der Alarme reagieren können. 2.516 Wagen wurden angehalten, 388 Personen festgenommen. Ein Drittel der Festgenommenen war ohne gültigen Führerschein unterwegs, ein weiteres Viertel der Festnahmen bezog sich auf sonstige Fahrzeug-Kriminalität (Fahrzeugdiebstahl, fehlende Versicherung, nicht bezahlte Steuern etc.). Seit der Nutzung der automatischen Fahrzeugnummernerkennung sei die Fahrzeug-Kriminalität im überwachten Gebiet um 10 % gesunken, außerhalb dieses Raumes aber leicht angestiegen. Wie bei der Videoüberwachung generell stellt sich daher auch bei der Fahrzeug-Erkennung die Frage nach einem Verlagerungseffekt.

Eine „eindrückliche“ Zahl von 1.662 Festnahmen realisierte ein 16-köpfiges Team in den West-Midlands bei 171 Einsätzen mit einem mobilen AFNES.[8] Davon entfielen 376 auf Diebstahl, 34 auf Raub, 27 auf Ein-

5 www.guardian.co.uk/archive/Article/0,4273,4143807,00.html
6 www.policereform.gov.uk/bureaucracy/Change_Proposal_Reports/Intelligence_Handling/ANPR/anpr.html
7 www.parliament.the-stationery-office.co.uk/pa/cm200102/cmhansrd/vo011102/text/11102w01.htm
8 www.policereform.gov.uk/bureaucracy/Change_Proposal_Reports/Intelligence_Hand page2.html

bruch, 200 auf Drogendelikte und 250 auf Fahrzeugkriminalität. In 2.000 Fällen seien Steuern nicht bezahlt gewesen. 64 gestohlene Fahrzeuge und Diebesgut im Wert von 500.000 Pfund wurden konfisziert.
Das Innenministerium und die Vereinigung der Polizeichefs feiern die automatische Nummernschilderkennung als Erfolg auf der ganzen Linie. Derzeit umfasst das Projekt Laser acht regionale Polizeien. Kurzfristig ist eine Ausdehnung auf insgesamt 21 vorgesehen. Erklärtes Ziel des Projektes ist es, für jede Polizei in England und Wales mindestens ein mobiles System zur Verfügung zu stellen. Der Einsatz soll sich aus den gesteigerten Einnahmen aus Geldbußen und Strafen selbst finanzieren.

Erfahrungen in der Schweiz

1998 startete die Schweizerische Polizeitechnische Kommission (SPTK), ein Dienstleistungsorgan der Konferenz der Kantonalen Polizeikommandanten, zusammen mit der Aargauer Kantonspolizei ein erstes Pilotprojekt. Im Baregg-Tunnel, einem Straßentunnel der Autobahn A1, wurden zwei Videokameras mit der Möglichkeit zur Fahrzeugnummernerkennung installiert. Die A1, die Bern und Zürich verbindet, ist eine der am stärksten befahrenen Straßen der Schweiz, das tägliche Verkehrsaufkommen im Baregg-Tunnel lag 2002 bei durchschnittlich 92.000 Motorfahrzeugen. Die Kameras schienen also gut platziert. Das AFNES wurde mit der nationalen Fahndungsdatenbank RIPOL verbunden.[9] RIPOL enthält u.a. die Daten der als gestohlen gemeldeten Fahrzeuge und der Halter von nicht versicherten Motorfahrzeugen. Ergab der Abgleich einen Treffer in der Datenbank, so wurde automatisch ein Streifenwagen alarmiert, der das Fahrzeug anhalten sollte. Falls sich keine Übereinstimmung ergab, wurden die Daten umgehend gelöscht. Wegen der sofortigen Löschung und dem eingeschränkten Einsatzgebiet erklärte der Eidgenössische Datenschutzbeauftragte denn auch das System für unproblematisch.[10]

Der Feldversuch dauerte 113 Tage und wurde danach eingestellt.[11] Die Erfolgsquote der Erkennung von Nummernschildern war mit 30 % sehr gering, was u.a. daran lag, dass Schweizer Kennzeichen unterschiedliche

9 Verordnung über das automatisierte Fahndungssystem (RIPOL Verordnung): www.admin.ch/ch/d/sr/1/172.213.61.de.pdf
10 www.edsb.ch/d/doku/jahresbericht/tb6/kap2.htm#16
11 Tages-Anzeiger v. 12.12.1998

Formate aufweisen und vielfach auch zweizeilig sind. Während des Versuchs gab es 500 Alarme, die in 262 Fällen einen Streifenwagen-Einsatz nach sich zogen. Bei den insgesamt 180 durchgeführten Kontrollen wurden 30 Auto- oder Nummernschilddiebe erwischt. Trotz der niedrigen Erkennungsrate von Fahrzeugnummern aus dem Pilotprojekt erließ die SPTK Ende 1999 eine Empfehlung an die Kantone zum Einsatz von automatischen Fahrzeugnummern-Erkennungssystemen.

Bereits im Mai 1999 hatte die Stadtpolizei Zürich einen zweiten Versuch gestartet – und zwar am Sihlquai, einem Punkt der Zürcher Innenstadt, den täglich rund 10.000 Autos passieren.[12] Sie verwendet dabei ein System der Firma CES namens Carsnap.[13] Es ist ebenfalls direkt mit RIPOL verbunden und meldet automatisch einen „Treffer", wenn ein gestohlenes Nummernschild oder das Kennzeichen eines gestohlenen bzw. unversicherten Fahrzeuges erkannt wird. Nur beim Vorliegen einer strafbaren Handlung werden Daten aufgezeichnet.[14]

Seit Dezember 2002 ist das System rund um die Uhr im Betrieb, wobei es innerhalb des ersten Monats gleich 45 Alarme gab. Dabei konnte die Polizei 20 Fahrzeuge anhalten und sieben Personen verhaften. 27 Autofahrer waren ohne Versicherungsschutz unterwegs, 12 hatten ihre Fahrzeuge nicht zur Kontrolle vorgeführt und fünf Personenwagen waren als gestohlen gemeldet.[15] Im März 2003 kaufte die Stadtpolizei für 85.000 Franken ein zweites System. Dieses ist mobil und kann deshalb überall in der Stadt eingesetzt werden.

Auch andere Kantone planen, automatische Fahrzeugnummern-Erkennungssystemen anzuschaffen. Die St. Galler Kantonsregierung hatte bereits einen positiven Beschluss gefasst, verzichtete dann aber aufgrund der erwarteten hohen Kosten und angesichts der schwierigen Haushaltslage auf die Anschaffung des Systems. Ganz abgeschrieben sind die Pläne jedoch nicht. Für einen späteren Zeitpunkt sucht man nach einer kostengünstigeren Lösung.[16]

„High-Tech-Fahndung" in Bayern und Hessen

12 Neue Zürcher Zeitung v. 20.3.2001
13 www.carsnap.ch
14 Gemeinderat Zürich, Prot. v. 22.1.2003, www.grzh.ch/2002/414.html
15 Tages-Anzeiger v. 22.2.2003
16 St. Galler Tagblatt v. 18.9.2003

Auch deutsche Polizeibehörden haben Interesse an AFNES-Systemen. Bayern startete im Herbst 2002 einen Versuch mit mobilen und fest installierten Systemen von fünf verschiedenen Firmen. Das Staatsministerium des Innern (StMI) nannte dabei drei Einsatzgebiete: Erstens sollte die Fahrzeugkennzeichen-Erkennung für Ringalarmfahndungen etwa nach Banküberfällen genutzt werden. Zweitens wollte man durch die Koppelung eines AFNES mit einer Radaranlage Geschwindigkeitsübertretungen feststellen und dabei gleichzeitig einen Abgleich mit Fahndungsdaten vornehmen; hierfür wurden zwei mobile Systeme und ein fest auf einer Autobahn-Schilderbrücke installiertes System getestet. Durch ebenfalls fixe Kameras an den Grenzübergängen Schirnding und Waidhaus-Autobahn an der EU-Außengrenze zu Tschechien wollte man drittens sämtliche ein- und ausreisenden Fahrzeuge mit dem Fahndungsbestand abgleichen. Für diesen letzten Bereich sah der Datenschutzbeauftragte keine rechtliche Grundlage.[17]

Rechtliche Grundlagen will Hessen mit einer Änderung des Sicherheits- und Ordnungsgesetzes schaffen. Hier spricht man offen von einer Nutzung dieser Technik für die Schleierfahndung.[18] Zwar würden die Daten nur gespeichert, wenn ein Abgleich positiv ist. Da als Einsatzzweck aber die „vorbeugende Bekämpfung“ von Straftaten mit erheblicher Bedeutung vorgesehen ist, könnte die automatische Nummernschild-Erkennung theoretisch auch zur Erstellung von Bewegungsbildern genutzt werden. Ob und in welchem Maße die Nummernschild-Erkennung zum Überwachungsinstrument wird, hängt von dem Datenbestand ab, mit dem sie gekoppelt ist.

Der polizeiliche Jubel über die „High-Tech-Fahndung“ verdeckt nicht nur die Gefahren für den Datenschutz. Die technische Weiterentwicklung brachte höhere Erkennungsraten und mit der Nutzung mobiler Systeme auch neue Einsatzmöglichkeiten. Die Nummernschilderkennung selbst verläuft zwar automatisch, die anschließende Verfolgung erfordert aber entsprechende personelle Ressourcen. Spätestens wenn Kamera-Standorte sich herumsprechen, dürften Verdrängungseffekte eintreten, die die Erfolge gegen die meist leichte Kfz-Kriminalität begrenzen. Nummernschild-Erkennungssysteme sind keine Wunderwaffen.

17 StMI: Presseerklärungen Nrn. 676 und 678/02 v. 22.11.2002

18 Hessisches Ministerium des Innern: Presseerklärung v. 19.11.2003

Daniel Boos wohnt in Zürich, ist Mitglied der Swiss Internet User Group (SIUG) und gehört zu den Organisatoren der Big-Brother-Awards Schweiz (www.bigbrotherawards.ch).

Jeden Tag Leben verteidigen

„Nicht-tödliche“ Waffen für Kriege und Innere Einsätze

von Olaf Arndt und David Artichouk

Mitte Mai dieses Jahres organisierte das Fraunhofer Institut für Chemische Technologie (ICT) eine hochkarätig besetzte Welt-Konferenz für Hersteller und Nutzer „nonletaler Waffen“(NLW). Die Tagung stellte eindrucksvoll unter Beweis, dass sogenannte „untödliche Wirkmittel“ die waffentechnische Zukunft für Polizei und Militär bedeuten könnten.

Pistolen, die Stromharpunen verschießen, Gewehre zum Abfeuern kleiner Gas-Tabletten und Markierfarben, Mikrowellenstrahler gegen Personen und Computer oder zu Barrieren umfunktionierte Airbagtechnik bieten eine hochgradig effektive zusätzliche Option bei Operationen von Sondereinheiten im Innern, im Kampf gegen gewaltbereite Bevölkerungsgruppen und vor allem bei Einsätzen im Krieg gegen den Terror. Das wurde an der Mammutveranstaltung des ICT in 32 Vorträgen und über 30 sogenannten „poster sessions“ demonstriert.[1]

Die Tagung fand etwas abseits in der Stadthalle des beschaulichen badischen Örtchens Ettlingen statt, das seinen an einem kleinen Fluss erbauten mittelalterlichen Stadtkern als „Traum an der Alb“ verkauft. Wie der Traum einer weniger gewalttätigen Zukunft, den die Spezialisten hier träumten, mit energiereichen Plasmatasern oder 160 mm Mörtelgranaten verwirklicht werden kann, wurde zwei Tage lang ausführlich diskutiert.

„Als träfe dich ein Vorschlaghammer, nur ohne bleibende Schäden“, sagt John B. Alexander, Vietnam-Veteran und geistiger Vater der „NLW“, über ihre Wirkung. Alexander, als Zugnummer prominent ins Programm

1 www.ict.fhg.de/english/events/nlw.html

platziert, tritt mit Rangers-Anstecknadel und Mosquito-Boots als Polit-Cowboy der Ära Bush für einen mit aller Härte geführten Kampf gegen den Terrorismus auf. Die von ihm propagierten Waffen erweitern das Spektrum, das konventionelle Waffen abdecken und schließen jene oft mit ein. Die Debatte um den exakten Begriffsgebrauch lässt den Widersinn offenkundig werden: „less lethal" ist schon einen Schritt näher dran an der „dualen Kapazität" (wahlweise umschaltbar von tödlich auf „weniger tödlich").

Auf dem Symposion zeigen 160 Wissenschaftler und Waffenfabrikanten aus 23 Ländern den anwesenden Militärs, Polizeispezialkräften und dem Fachpublikum, wie man mit Gas, Schall, Strom und Licht gezielt Terroristen, revoltierende Gefangene oder Randalierer ausschalten kann. Dass „nicht letale Wirkmittel" keinesfalls zu sorglosem Gebrauch einladen und sich nicht immer im Einklang mit bestehenden Gesetzen befinden, machen die Vorträge kritischer Wissenschaftler, Juristen und des Roten Kreuzes deutlich.

Anwesende Vertreter von Nichtregierungs-Organisationen und Friedensforscher gehen noch weiter. Sie sehen in „mass incapacitation tools", Mittel zum flächendeckenden Behandeln größerer Gruppen von Menschen, schlicht Folterwerkzeuge in einer neuen Dimension. Ein oft zitiertes Beispiel für die Vorzüge untödlicher Wirkmittel ist die Moskauer Musical-Theater-Belagerung im letzten Winter. Nach Ansicht der meisten Vortragenden eine gelungene Aktion. Denn ohne den Gaseinsatz, so behaupten sie, wäre die Zahl der Todesopfer vermutlich noch höher ausgefallen. Ein Gefühl beschleicht den kritischen Zuhörer: dass der Waffenmarkt die Heimat des hinkenden Vergleichs ist. Konventionelle Waffen haben statistisch bewertet im Schnitt keine verheerendere Wirkung als das viel gepriesene Moskauer Gas. 179 Tote (davon 129 Geiseln) – 20 Prozent der Personen, die sich in dem Theater aufhielten – sind ohnedies keine Werbung für ein Programm, das „relativ reversible" Schäden verspricht.

„Das Recht auf Respekt vor dem Leben" müsse als Summe hinter allen Überlegungen stehen, fordert folgerichtig ICT-Chef und Gastgeber Klaus-Dieter Thiel.

Aufforderung zum Tanz

Es ist grundsätzlich kein schlechter Traum, Entführer, Bankräuber und Randalierer nicht gleich mit der letalen Dosis behandeln zu müssen. Vor

allem im inneren Einsatz, wo Kollateralschäden komplexere Folgen haben, bergen die neuen Waffen, die heute technisch noch in den Kinderschuhen stecken, hoffnungsvolle Aspekte für die polizeilichen Anwender. Die Abwägung zwischen Festnahmedringlichkeit und dem Überleben des vermeintlichen Täters fällt weg. Im Ernstfall steht die althergebrachte tödliche Schusswaffe dem Beamten weiterhin zur Verfügung.

Aber verlangt das größere Spektrum an Möglichkeiten nicht nach einer verbesserten Ausbildung? Welche Waffe in welcher Situation ziehen? Elektro-Taser, Fangnetz, Mikrowellenkanone, Gummigeschoss oder doch besser die Gaspistole? Alles lösbare Probleme, sagen die anwesenden Polizeipraktiker und Vertreter der Herstellerfirmen – bevor sie sich in Lobbyisten verwandeln und ein trauriges Lied von der Mühsal der Überzeugungsarbeit bei den Entscheidungsträgern anstimmen. Es klingt nach leeren Kassen, komplizierten Strukturen und der Angst vor öffentlichen Diskussionen. Neue Polizeibewaffnung „muss ja immer gleich politisiert werden".

Die Russen sind angesichts der ängstlichen Nachfragen ihrer westeuropäischen Kollegen oft perplex. Die Amerikaner lächeln. Schneller als die Europäer haben sie die Vorteile der nicht-letalen Waffen im strategisch-politischen Bereich erkannt. Es sind klinisch saubere Waffen. Sie fügen sich nahtlos in die Philosophie der chirurgischen Eingriffe moderner Kriege ein, die komplette Operation mit Anästhesie.

Früher galt „Tötet sie alle. Gott wird die Seinen erkennen". Heute, im Zeitalter der Kriege, die Befreiung von Diktatur versprechen, tritt das technische Vermögen, die zielgenaue High-Tech-Waffe, an die Stelle des Glaubens. Jetzt kann dank nicht-letaler Wirkstoffe Genauigkeit mit Gründlichkeit erfolgen, konkret zum Beispiel durch ein nur auf spezifische Bevölkerungsgruppen wirkendes Gas. Die Unseren werden wir hinterher retten können. Die Selektion zwischen angepeiltem Ziel und dem uninteressanten oder schützenswerten Rest ist bei nicht-letalen Waffen erheblich preiswerter. John B. Alexander demonstriert das in seinem Vortrag mit Hilfe einer Differentialgleichung. Seine Mathematik für Militärs errechnet, dass das Gefühl persönlicher Sicherheit einen direkten Einfluss auf die Ökonomie haben wird. Ob es zu einer größeren Proliferation führt oder, im Gegenteil, diese Waffen in einer wirtschaftlichen Sackgasse enden, werden wir abwarten müssen.

In Ettlingen bleibt unübersehbar, wenngleich unausgesprochen, dass Strahlen, Ströme und Chemikalien zum Zauberstab der Neuen Weltordnung verschmelzen könnten. Die nach seiner Rede in West Point im Juni

2002 „Bush-Doktrin“ genannten Optionen im weltweiten Krieg gegen den Terror, also vor allem Präventivschläge gegen Extremistengruppen im Ausland und Strafaktionen gegen tatsächliche und vermutete Unterstützerstaaten, scheitern sicher nicht an mangelnder militärischer Schlagkraft. Die eigentliche Wirkungskraft nicht-letaler Waffen ist die Verheißung auf politische Durchsetzbarkeit geplanter Operationen. Das sind die Argumente: Unbeteiligte werden weitgehend geschont. Vor allem im urbanen Raum, dem bevorzugten Feld von Terroristen, ist das bislang nicht gewährleistet. Die Aktionen sind schneller, leiser, sauberer, auch umweltfreundlicher und billiger. Die überlebenden Terroristen und Despoten könnten auf diese Weise den Gerichten zugeführt werden.

Stilvolle Sozialingenieure

Noch eindrucksvoller als das Bildmaterial von Testreihen und Einsätzen der Waffen sind in vielen Fällen die Anbieter und Experten selbst. Elegante Nadelstreifendreiteiler, maßgeschneiderte Designerschuhe und Hemden mit eingestickten Firmenlogos vermitteln den Eindruck stilvoller Sozialingenieure. Der graue Waffenschmied im Stangenanzug scheint ausschließlich in Deutschland überlebt zu haben.

Das gleiche Bild kehrt in den Präsentationen wieder. Die ehemaligen Kanonenbauer von Rheinmetall krökeln sich mit bemühter Verve („we can do better“) durch eine Powerpoint-Präsentation für ihren Plasma-Taser, der gleich ganze Menschenmengen per Stromschlag umhauen soll.[2] Die amerikanischen Konkurrenten kommen dagegen mit DVDs von der Produktionsqualität eines „X-men“ Trailers auf die Bühne. Thomas P. Smith stellt sein Produkt „Advanced Taser®“ als Joystick für den Polizisten vor, ein smartes Gerät für den geschmackssicheren Einsatz. Smith hat mit schwungvollem Filzstiftstrich auf seinem Namensschild die Aussage auf drei Buchstaben reduziert: Tom ist dein Ansprechpartner. Das hat Tradition; der Erfinder Jack Cover hat das Produkt-Akronym aus den 50er Jahre Future-Comics abgeleitet. Taser bedeutet: „Tom A. Swift Electrical Rifle“ und ein frühes Modell hieß „Tron“. So kehren die Namen der Helden wieder, in Disneys und in unserer Welt.

Tom ist der dunkle Messias, der mit dem Stromschlag straft. Der eloquente Präsident von Taser International, der momentan wohl erfolg-

2 www.telepolis.de/deutsch/inhalt/co/14971/1.html

reichsten Schockwaffenfirma aus Arizona, „verteidigt täglich Leben“ mit seinem Bestseller „M26“.[3] M26 ist eine Druckluftpistole, die 50.000 Volt an zwei Strom führenden Kabeln auf 7 Meter Distanz mit einer Miniaturharpune in den Angreifer jagt und diesen bereits nach einer halben Sekunden umwirft. Der Strom aus 8 Mignon-Batterien durchschlägt 6 cm Kleidung und Leder und lässt den bereits kampfunfähigen Delinquenten, laut Prospekt ein aggressiver Vollbartträger mit Holzfällerhemd und hoch erhobenem Radmutterschlüssel, noch weitere 5 Sekunden lang den Saft schmecken, der ihn niederstreckt. Danach wird der Beschossene eine Zeit lang Probleme haben, seine Muskeln unter Kontrolle zu halten, aber das vergeht. Zurück bleiben zwei Einstichlöcher von den Polen, groß wie Insektenstiche. Eine Erfahrung, die von 40.000 Freiwilligen trotz hoher Belohnung keiner ein zweites Mal machen wollte.

Ganz in schwarz, in hautengem Rollkragenpullover, zelebriert Tom eine Messe zwischen Blumenbuketts: Reverend Taser, wie er selbstironisch beim Pausengespräch bemerkt. In seinen Videos knicken die stärksten Männer der Welt um wie Halme im Wind. Überall fallen Freiwillige und weniger Freiwillige. Eine kaum gestellt wirkende Szene zeigt in Überwachungskamera-Ästhetik einen nackten Gefangenen, der in seiner Zelle getasert wird. Von Drogen aufgepeitschten Randalierern und flüchtenden Gangstern wird keine Chance gegeben. Alle fallen, fallen und winden sich.

Das neue Modell weist sich durch ein X in Terminator-Flüssigmetall-Typographie bereits im Layout als Science-Fiction-Waffe aus. Die X26 ist neongelb, 60 % leichter als ihre Vorgänger, mit Flash-LEDs und Laserpointer ausgerüstet. 105 Schuss Kapazität, Pulsweitenmodulation, Feuerdaten-Download Port, ergonomischer Griff. Die „neue Dimension der Gesetzesvollstreckung“ ist mit einem „Exoskeleton“ genannten „Blade Tech® Paddle“-Halfter lieferbar. Optional: eine Doppel-DVD mit Videotrainingsprogramm. Da reimt sich einfach alles: die X26 ist so frappierend brillant in Szene gesetzt, dass man Mühe hat, sich statt Keanu Reeves den Polizei-Einsatzleiter mit der exotischen Waffe in der Hand vorzustellen.

Eine aggressiv klare, und verflucht coole „Men-in-Black“-(!)-Kampagne vermarktet die perfekte Waffe. Sie ist „clean“ und sie sieht schick aus. Sie ist garantiert untödlich, digital kontrolliert, enorm effektiv und

3 www.taser.com

kostet etwa 1.000 Euro. Jeder Mann muss eine haben wollen. Tom ist angetreten, um den Erfolg öffentlich zu performieren. Aus einer Spezialinnentasche seines Taser-Anzugs fliegen Visitenkarten auf den Kreis der Kunden zu wie die Kugeln der Agenten in „Matrix“ – man kann sie einzeln aus der Luft pflücken. Kunde: „Ich komme aus Korea und habe aus Ihrem Vortrag verstanden, dass sie nicht nach Asien exportieren dürfen... was kann man tun?“ Tom: „Unser Sales Representative in Malaysia wird sich um Ihre Anfrage kümmern.“

Tom weiß, wie er ins Rampenlicht treten muss – er ist halb Art Director, halb Propagandaminister. Auf der Konferenz analysiert er messerscharf die Resultate von 2.000 Einsätzen: keine Probleme mit Herzschrittmachern, die setzen kurz aus, aber nicht in gesundheitsschädlichem Umfang. Keine Probleme mit der Muskelelastizität, die kommt wieder. Drogenkuriere mit geplatzten Heroinbeuteln im Magen sterben nicht am Taser, sondern am Stoff. Keine Aussage ist länger als neun Sekunden, dann ertönt das knallhart skandierende „next slide“.

Jede Frage wird mit weniger als vier Sätzen beantwortet. „Todesfälle im Zusammenhang mit dem Einsatz von M26 sind uns nicht bekannt. Wir sind stark an Dokumenten über angebliche Fälle interessiert. Wir werden sie unabhängigen medizinischen Gutachtern zur Prüfung übergeben.“ Nebensätze existieren nicht. Zweifel ebenso wenig. Die humane Waffe ist erfunden.

In den USA ist sie bei 2.500 Police Departments eingeführt. 250 haben sämtliche Beamte damit ausgerüstet. Taser International verleiht als zusätzlichen Anreiz jährlich die Medaille für „untödlichen Heroismus“ an denjenigen Polizisten, der selbst in größter Gefahr konsequent zur Stromwaffe greift, um die Suspekten zu schonen. Im April 2001 empfahl die deutsche Innenministerkonferenz den Bundesländern die Anschaffung für die Sondereinsatzkommandos: Drei Länder – Berlin, Sachsen und Nordrhein-Westfalen – haben das Modell seit einem Jahr im Testeinsatz, fünf weitere haben sie bereits gekauft, alle hadern aber noch wegen Zulassungsproblemen, sie in den Regeldienst zu übernehmen. Großbritannien hat einen Schwung geordert, der in fünf ausgewählten Distrikten eingesetzt wird. Die Schweizerische Polizeitechnische Kommission (SPTK) gab im Juli dieses Jahres ihr Placet. Zwei Kantonspolizeien – Basel-Land und Schwyz – hatten die Waffe bereits vorher angeschafft. Nach der SPTK-Empfehlung entschlossen sich Stadt- und Kantonspolizei Zürich zu einem Testlauf, die restlichen helvetischen Polizeikorps dürften in Kürze nachziehen. Frankreich und Spanien sind in Lau-

erstellung: Man evaluiert derzeit die vielfältigen Implikationen der Anwendung. Im Auftrag des amerikanischen Verteidigungsministeriums forschen Taser International an einer aufgerüsteten Version mit 100 Meter langem Draht. Wozu? Erfolgreiche Einsätze gegen Selbstmörder und Randalierer auf Hausdächern zeigen das Potential, die X26 auch im Kampf gegen Terroristen einzusetzen. Dafür wird jedoch mehr Reichweite benötigt.

Eine Consumer-Variante, im Volksmund „Dog-Taser" genannt, ist in den USA frei erhältlich und geeignet, Attacken von Kampfhunden abzuwehren. Es ist nur von einem Fall bekannt, dass ein Tier nicht sofort das Weite suchte. Es war ein Experiment. Der Hund sollte ein Kind in einem Raum bewachen. Nach dem vierten Schuss hat er sich in eine Ecke verzogen und „tot gestellt".

John B. Alexander weiß zu berichten, dass ihm im Selbstversuch mit Klebeelektroden der Taser die Kappe der Armeestiefel durchschlagen hat. Seinem 16-jährigen Sohn Josh hat Alexander erlaubt, den „Büffel zu reiten" und die Waffe an sich selbst zu testen. Obwohl extrem körperlich fit und wahrlich kein „couch potatoe", habe der Taser Josh im Nu aus dem Sattel gehauen, berichtet der Vater schmunzelnd.

Das makabre Beispiel stellt noch einmal klar heraus: Was heißt schon non-letal? Ein bisschen weniger tot? Wenn man Glück hat, wie Tom und Josh, und kerngesund ist. Denkt man jedoch an die intendierten Einsätze, steht eher zu bezweifeln, dass die Gegner sich in Topform befinden und die Anwendung so gut vertragen wie die Marine Corps-Hünen, die in Ettlingen kaum zwischen die Tischreihen passen.

Der D-Modus

Die Euphorie der Ettlinger Elite wird zur Zeit noch durch zahlreiche juristische Probleme gebremst. Genau genommen sind die meisten Waffen heute schlicht verboten. Selbst in Deutschland ist der Taser-Einsatz ein rechtliches Problem. Viele der Waffenkonventionen des 20. Jahrhunderts ächten nicht-letale Waffen, in den meisten Fällen zum Schutz der Soldaten vor unnötigen Qualen.

So wurde der Kriegseinsatz von Reizgasen nach den Erfahrungen des Ersten Weltkrieges 1925 im Genfer Protokoll verboten. Seit 1993 liegt ein Bann auf ätzenden, klebenden, einschläfernden und in anderer Form die Rechte des freien Bürgers einschränkenden Mitteln. Dass mit Gasen im Polizeieinsatz gegen Demonstranten seit Jahrzehnten „sehr gute" Erfah-

rungen gesammelt werden, rief die Militärs auf den Plan. Beim Ausräuchern der Taliban in ihren Höhlen, das zeigt Viktor Selivanov von der Baumann Universität Moskau in einer humorvoll aufbereiteten Flash-Animation, die den ganzen Saal zum Lachen bringt, wäre Gas die ideale Waffe gewesen.

Schon arbeiten Juristen am gleichen Recht für alle. Anstatt das Naheliegende zu tun, und das teilweise restriktivere Kriegsrecht für das Polizeirecht einzufordern, finden sich offenbar ausreichend Juristen bereit, internationales Recht und die zahlreichen Konventionen auf neue Mindeststandards hin durchzuforsten. Zwar können Konventionen schwerlich andere ersetzen, ein juristisches Problem! Aber es wird bereits an kreativen Lösungsansätzen gearbeitet.

In Ettlingen endete der Kongress mit einem Vorschlag der Juristen aus der „European Working Group" unter Leitung von Friedhelm Krüger-Sprengel, International Society for Military Law: Die behutsame Annäherung der „EWG" an die Zulassung bislang verbotener Wirkstoffe ist der Beginn einer Suche nach einer Klassifizierung der neuen Technologie jenseits der Genfer Vereinbarungen.

Wir, die „bio-specimen", Exemplare aus der weichen Kollektion der Humanoiden, warten derweil im „D-Modus" auf die Wunder aus den neuen Waffen. Wir werden detektiert (detect), weggehalten (deny), ausgesondert (discriminate), verzögert (delay), verteidigt (defend), geblendet (dazzle), besiegt (defeat) und nur im ärgsten Fall zerstört (delete/destroy).

Olaf Arndt und David Artichouk arbeiten seit 1989 mit der interdisziplinären Künstlergruppe „Beobachter der Bediener von Maschinen" BBM (www.bbm.de) an Recherche-Projekten und Technologiekritischen Installationen, so genannten Maschinen-Performances.

Rechtshilfe ohne Rechtsschutz

Rechtshilfe- und Auslieferungsabkommen mit den USA

von Hartmut Wächtler

Gummiweiche Formulierungen und ein weitgehender Verzicht auf Datenschutzprinzipien und Rechtsschutzmöglichkeiten kennzeichnen die neuen Abkommen zwischen der EU bzw. Deutschland und den USA.

Der 11. September 2001 hat eine rasante rechtspolitische Entwicklung nach sich gezogen. Wie rasant sie war, zeigt sich sehr deutlich an den Vereinbarungen zwischen Europol und den US-Behörden. Am 6. Dezember 2001 schlossen sie ein erstes Abkommen, das sich noch auf den Austausch von strategischen, d.h. nicht-personenbezogenen Informationen beschränkte. In dessen Art. 3 gab es jedenfalls den Versuch, den Datenaustausch auf bestimmte Kriminalitätsbereiche zu limitieren. Art. 10 II stellte bereits weitere Vereinbarungen zum Austausch personenbezogener Daten in Aussicht. Dem sind die Parteien ein Jahr später gefolgt. Im Zusatzabkommen vom 5. Dezember 2002 gibt es keine Begrenzung der Kriminalitätsbereiche mehr.[1] EUROPOL kann danach die bei ihm vorhandenen Informationen auf Anfrage oder spontan an die USA übergeben. Die Einschränkungen für die Datenübermittlung sind äußerst vage gehalten. So heißt es in Art. 5 Nr. 1a:

> „Die Übertragung von Informationen gemäß dem vorliegenden Abkommen und deren weitere Verarbeitung durch die empfangende Partei muß dem in der Anfrage geäußerten Zweck entsprechen, der die Verhütung, Aufdekkung, Ermittlung und Strafverfolgung jedweder spezifischer Straftaten sowie jegliche spezifische Analysezwecke einbezieht, auf die sich diese Informationen beziehen. Falls eine der Parteien die Verwendung solcher Informationen für andere Zwecke wünscht, beantragt sie zuvor die schriftliche Zustimmung der Partei, die die Informationen bereitgestellt hat."

1 EU-Ratsdok. 15231/02 v. 5.12.2002

Hinsichtlich der besonders sensiblen Informationen heißt es in Art. 6:

> „Personenbezogene Daten, die Hinweise auf die rassische Herkunft, politische Anschauungen oder religiöse oder andere Überzeugungen oder Gesundheit oder Sexualleben geben, dürfen nur geliefert werden, nachdem die übermittelnde Partei festgestellt hat, dass diese Daten für einen der in Art. 5 I aufgeführten Zwecke von besonderer Bedeutung sind."

Mit dieser Formulierung wurde der Rahmen der entsprechenden EUROPOL-Verordnungen verlassen, wonach eine solche Übermittlung nur zulässig ist, wenn dies „absolut notwendig" ist. Ein zusätzlicher Briefwechsel sollte diesen „Schönheitsfehler" offenbar ausgleichen.[2] Darin ist unter Punkt 6 ausgeführt, dass der Ausdruck „von besonderer Bedeutung" im gleichen Sinne zu verstehen sei, wie die in den EUROPOL-Verordnungen verwendete Formel „absolut notwendig". Weshalb nicht gleich im Abkommen selbst Klarheit geschaffen wurde, ist völlig unklar.

Für den deutschen Leser und potentiellen Datenlieferanten stellt sich vor allem die Frage, wie er selbst einen Missbrauch seiner Daten, die via EUROPOL an die USA geliefert werden, verhindern kann. Hier ist zunächst Art. 3 III des Zusatzabkommens einschlägig:

> „Das vorliegende Abkommen dient ausschließlich dem Zweck der Zusammenarbeit der Parteien. Aus den Bestimmungen dieses Abkommens leiten sich weder Ansprüche von Privatpersonen ab, Beweise zu erlangen, zu unterdrücken oder auszuschließen oder die Bearbeitung einer Anfrage zu verhindern, noch stellt es eine Abweichung von jedwedem bereits vorhandenen diesbezüglichen Recht einer Privatperson dar."

Dies soll wohl heißen, dass sich keine Individual-Ansprüche auf Verhinderung der Datenübermittlung aus dem Zusatzabkommen ableiten lassen sollen. Das Übereinkommen enthält keinerlei eigenständige Bestimmungen über den Datenschutz. Art. 5 III verweist auf die „angemessenen Sicherheitsmaßnahmen, gemäß dem innerstaatlichen Recht". Allerdings gibt es in dem gesamten Zusatzabkommen keinerlei Vorschriften darüber, dass die Person, deren Daten übermittelt werden, von der Übermittlung überhaupt etwas erfährt.

Wenn umgekehrt eine Privatperson bei der empfangenden Stelle Auskunft darüber begehrt, welche Daten über sie übermittelt worden sind, muss gemäß Art. 10 I die empfangende Partei die übermittelnde Partei zu Rate ziehen. Nach Art. 10 II werden die Informationen nicht an die Privatperson herausgegeben, wenn die übermittelnde Partei ihre

2 Briefwechsel zu FN 1: EU-Ratsdok. 15231/02 ADD 1 v. 5.12.2002

Zustimmung nicht erteilt. Beschreitet nun die Privatperson den Rechtsweg gegen diese Nicht-Freigabe von Informationen,

> „wird die empfangende Partei mit allen in ihrer Macht stehenden Rechtsmitteln die diesbezüglichen Interessen der übermittelnden Partei durch Beratung, Unterstützung und Erscheinen vertreten."

Im Klartext heißt dies, dass die empfangende Partei durch alle Instanzen Auskunftsverlangen von Betroffenen abwehren muss, wenn die übermittelnde Stelle die Informationen nicht freigibt – und zwar auch dann, wenn nach innerstaatlichem Recht der empfangenden Partei die Information an sich freigegeben werden müsste.

Angesichts dieser vertrackten datenschutzrechtlichen Situation wird man Personen, die davon ausgehen müssen, dass ihre Daten bei EUROPOL gespeichert werden, zukünftig den Rat geben müssen, vorbeugenden Rechtsschutz gegen die Übermittlung ihrer Daten von den nationalen deutschen Behörden an EUROPOL in Anspruch zu nehmen. Da wegen des Zusatzabkommens mit den USA weder der weitere Datenweg verfolgbar noch eine ausreichende Zweckbindung gewährleistet ist – von einem Rechtsschutz ganz zu schweigen –, dürfte die Übermittlung personenbezogener Daten von deutschen Behörden an EUROPOL jedenfalls mit deutschem Datenschutzrecht kaum mehr in Übereinstimmung zu bringen sein. In diesen Zusammenhang passt auch, dass man sich bei der Aushandlung des Zusatzabkommens nicht einmal an die eigenen Vorgaben gehalten hat. 1999 hatte der Rat die „Bestimmungen über die Übermittlung von personenbezogenen Daten durch Europol an Drittstaaten und Drittstellen" beschlossen.[3] Gemäß deren Art. 7 hat EUROPOL sicherzustellen, dass der Empfänger sich verpflichtet, die empfangenen Daten zu berichtigen oder zu löschen, wenn sich herausstellt, dass sie unrichtig, ungenau oder überholt sind oder nicht hätten übermittelt werden dürfen. Eine entsprechende Festlegung fehlt in dem Zusatzabkommen mit den USA. Dort heißt es in Art. 9 III lediglich, dass in diesem Fall die empfangende Partei alle „angemessenen Maßnahmen" ergreifen soll. Dies „kann die Ergänzung, Löschung oder Berichtigung dieser Informationen einschließen."

Dies ist das Gegenteil dessen, was noch 1999 verbindlich festgelegt worden war. Ebenso fehlt es an der Verpflichtung des Empfängers, die empfangenen Daten zu löschen, wenn sie für die Zwecke, für die sie

3 Rechtsakt des Rates vom 12.3.1999, in: Amtsblatt der EG Nr. C 88 v. 30.3.1999, S. 1

übermittelt wurden, nicht mehr erforderlich sind. Auch dies war in Art. 7 III der Bestimmungen von 1999 noch enthalten. Schließlich fehlt in dem Abkommen mit den USA jede Vereinbarung über einen verantwortlichen Haftungsträger im Fall einer unbefugten oder unrichtigen Datenverarbeitung. Dies dürften weitere Argumente für jeden Kläger sein, der die deutschen Behörden daran hindern will, seine Daten an EUROPOL zu übermitteln, wenn nur die mindeste Gefahr besteht, dass sie von dort in die USA weitergereicht werden könnten.

Menschenrechte und Auslieferung

Ein halbes Jahr nach dem Zusatzabkommen mit Europol nahm der Rat das Auslieferungs- und das Rechtshilfeabkommen mit den USA an.[4] Die beiden Verträge, so erklärten die Minister, böten „die notwendigen Garantien für den Schutz der Menschenrechte und Grundfreiheiten und die Einhaltung der Verfassungsgrundsätze der Mitgliedstaaten." Bei dieser Bewertung sind Zweifel angebracht.

Das Abkommen über die Auslieferung ermöglicht diese sowohl zur Strafverfolgung als auch zur Strafvollstreckung, wobei die Erheblichkeitsschwelle für die auslieferungsfähigen Straftaten so niedrig angesetzt ist, dass in der Praxis der Betroffene bei jeder Art von Straftat ausgeliefert werden kann. Von der Fachöffentlichkeit beobachtet wurde vor allem, ob sich die EU in den Fragen Auslieferung bei Todesstrafe und/ oder an eine Sondergerichtsbarkeit sowie in der Frage des Datenschutzes hat durchsetzen und ihre Grundsätze wahren können.

Zum überwiegenden Teil ist dies nicht gelungen. Art. 13 des Auslieferungsabkommens räumt dem ersuchten Staat die Möglichkeit ein, Auslieferung nur unter der Bedingung zu gewähren, dass die Todesstrafe gegen die auszuliefernde Person nicht verhängt wird oder jedenfalls nicht vollstreckt wird. Dies gibt der europäischen Seite immerhin die Möglichkeit, in solchen Fällen die Auslieferung zu verweigern.

Für den Fall, dass dem Auszuliefernden ein Verfahren vor einer Sondergerichtsbarkeit – konkret: einem Militärtribunal – droht, sieht das Abkommen keine entsprechende Weigerungsklausel vor. Art. 17 II bietet stattdessen eine gummiweiche Konsultationspflicht bei Fällen, „in denen die Verfassungsgrundsätze des ersuchten Staates oder die für diesen ver-

4 EU-Ratsdok. 9153/03 v. 3.6.2003 und 9845/03 v. 5./6.6.2003

bindlichen endgültigen richterlichen Entscheidungen ein Hindernis für die Erfüllung seiner Auslieferungspflicht darstellen können.“ Was geschehen soll, wenn die vorgeschriebenen Konsultationen keinen Erfolg haben, wird nicht geregelt.

Das Rechtshilfeabkommen

Das Rechtshilfeabkommen enthält in Art. 4 die Verpflichtung des ersuchten Staates, die Bankverbindungen und darüber hinaus sämtliche finanziellen Transaktionen von juristischen oder natürlichen Personen zu übermitteln, die einer Straftat verdächtigt, wegen einer solchen angeklagt oder, wie es heißt, „verurteilt oder in sonstiger Weise in Straftaten verwickelt“ sind. Nach deutschem Recht fallen nur ausgesprochene Bagatelldelikte nicht unter die Auskunftspflicht nach dieser Vorschrift. Eine Generalklausel mit Bezug zu terroristischen Aktivitäten und zur Geldwäsche weicht diese mögliche Begrenzung weiter auf.

Art. 5 erlaubt gemeinsame Ermittlungsteams, wenn dies für zweckmäßig gehalten wird. Die Teams sollen in jedem Land, das darin vertreten ist, Ermittlungsmaßnahmen veranlassen, ohne dass die übrigen Staaten ein Rechtshilfeersuchen einreichen müssen. Nach Art. 5 IV des Abkommens sollen sich die Ermittlungen stattdessen auf die jeweiligen innerstaatlichen Rechtsnormen des betreffenden Staates stützen.

Eine Regelung wie beim Auslieferungsabkommen, dass keine Rechtshilfe geleistet werden muss, wenn in dem betreffenden Strafverfahren die Todesstrafe droht, sucht man im Rechtshilfeabkommen vergeblich. Im Gegenteil: nach Art. 9 II b darf der ersuchte Staat für die Bereitstellung von Beweismitteln und Informationen „keine allgemeinen Einschränkungen mit Blick auf die Rechtsnormen des ersuchenden Staates für den Umgang mit personenbezogenen Daten auferlegen.“

Gleiches gilt für den zweiten Prüfstein, ob nämlich Rechtshilfe verweigert werden kann, wenn die Informationen in Sondergerichtsverfahren verwertet werden sollen. Auch hier gibt es keine Regelung. Als mögliches Schlupfloch ist wohl Art. 13 zu verstehen, der dem ersuchten Staat die Ablehnung der Rechtshilfe ermöglicht, wenn „durch die Erledigung des Ersuchens die Souveränität, die Sicherheit, die öffentliche Ordnung und andere grundlegende Interessen dieses Staates beeinträchtigt würden.“ Möglicherweise hat man hier, um die US-Seite nicht zu reizen, auf eine deutlichere Ausgestaltung des Vertragstextes verzichtet. Wohin das führt, bleibt abzuwarten.

Art. 9 kann als eine Art Zweckbindungsklausel verstanden werden. Als Verwendungszweck sind vor allem kriminalpolizeiliche Ermittlungen und Strafverfahren sowie Bedrohungen der öffentlichen Sicherheit des ersuchenden Staates aufgeführt. Für andere als die aufgeführten Zwecke dürfen die übersandten Daten nach Art. 9 I e nur mit vorheriger Zustimmung des ersuchten Staates verwandt werden. Echte Beruhigung kann diese Vorschrift jedoch nicht verbreiten, da überhaupt nicht geklärt ist, wie die Einhaltung dieser Zweckbindungsvorschriften überwacht werden soll. Die Konsultationsvorschrift des Art. 11 dürfte jedenfalls für eine effektive Kontrolle nicht ausreichen, zumal in einer erläuternden Note zwischen den Parteien hinsichtlich der Zweckbindung in Art. 9 noch einmal ausdrücklich festgehalten worden ist, dass für die Ablehnung der Rechtshilfe Datenschutzgründe nur in Ausnahmefällen geltend gemacht werden dürfen. Eine bemerkenswerte Klarstellung.

Rechtshilfevertrag zwischen Deutschland und den USA

Am 14.10.2003 unterzeichneten Bundesjustizministerin Zypries und ihr US-Kollege Ashcroft zusätzlich ein bilaterales Rechtshilfeabkommen.[5] Sachlich erstreckt sich dieses auf strafrechtliche Verfahren einschließlich Steuerstraftaten, Ordnungswidrigkeiten nach dem deutschen Kartellrecht und unter bestimmten Voraussetzungen selbst auf einfache Ordnungswidrigkeiten. Die Rechtshilfe erstreckt sich auf die Fahndung nach und Identifizierung von Personen oder Gegenständen, die Zustellung von Urkunden, die Abnahme von Aussagen oder anderen Erklärungen, die Überstellung von Häftlingen z.B. zur Zeugenaussage, die Überlassung von Urkunden o.ä., die Durchsuchung und Beschlagnahme und besondere Ermittlungsmethoden wie die beispielhaft erwähnte Überwachung des Fernmeldeverkehrs, verdeckte Ermittlungen und kontrollierte Lieferungen. Schließlich wird die Unterstützung bei Verfahren in Bezug auf Sicherstellung und Einziehung von Vermögenswerten und die Beitreibung von Geldstrafen sowie in einer Generalklausel jede andere Form der Rechtshilfe, die nicht nach dem Recht des ersuchten Staates verboten ist, zugesichert. Die Rechtshilfe ist – von Ausnahmen abgesehen – nicht davon abhängig, dass die Handlung, deretwegen sie betrieben wird, in beiden betroffenen Staaten verfolgt wird (Art. 1 IV).

5 bisher nicht veröffentlicht

Auch dieses Abkommen sieht keine Klausel vor, dass Rechtshilfe verweigert werden kann, wenn in den USA die Todesstrafe oder ein Sondergerichtsverfahren drohen. In Art. 3 ist jedoch eine Generalklausel enthalten. Danach kann Rechtshilfe verweigert werden, „wenn die Erledigung des Ersuchens die Souveränität, die Sicherheit oder andere wesentliche Interessen des ersuchten Staates beeinträchtigen würde." Auch hier kann vermutet werden, dass politische Rücksichtnahme auf die USA dazu geführt hat, weder Sondergerichte noch Todesstrafe beim Namen zu nennen.

Art. 10 regelt die Vernehmung von Zeugen im Rechtshilfeweg. Verfahrensbeteiligten, z.B. Verteidigern, ist die Anwesenheit bei der Zeugenbefragung gestattet, jedoch nur, wenn sie im Rechtshilfeersuchen genannt werden. Sie haben kein eigenes Fragerecht, sondern nur das Recht, Fragen an die aussagende Person vorzuschlagen. Durchsuchungen und Beschlagnahmen sind nur zulässig, wenn sie auch nach dem Recht des ersuchten Staates möglich sind (Art. 11 I Nr. 2). Gleiches gilt für die erwähnten besonderen Ermittlungsmethoden in Art. 12.

Ein besonderes Kapitel sind auch hier die Datenschutzbestimmungen bzw. deren Restbestände. Zunächst enthält Art. 9 II die Vorschrift, dass der ersuchte Staat Unterlagen oder sonstige Informationen, die sich im Besitz einer Regierungsstelle oder Behörde befinden, aber nicht öffentlich zugänglich sind, „in dem selben Umfang und unter den selben Bedingungen zur Verfügung stellt, wie sie seinen eigenen entsprechenden Behörden zugänglich wären."

Diese Bestimmung ist deswegen bemerkenswert, weil damit den Behörden des ersuchenden Staates dieselbe Rechtsstellung beigemessen wird wie den innerstaatlichen Behörden, ohne dass der Bürger, dessen Informationen auf diese Weise verarbeitet werden, die Möglichkeit hätte, sich in einer entsprechenden Weise zu wehren. Es ist nicht erkennbar, wie ein deutscher Staatsangehöriger sich z.B. zur Wehr setzen soll, wenn eine deutsche Polizeibehörde seine Informationen an eine ähnliche Behörde in den USA weitergibt. In Deutschland könnte er dies unter den Bestimmungen des deutschen Datenschutzrechtes und auf dem üblichen Verwaltungsrechtsweg. Geschieht die Weitergabe seiner Daten auf dem Rechtshilfeweg in die USA, fehlt es an jeder realistischen Möglichkeit des Rechtsschutzes. Dies um so mehr, als in Art. 1 VI ausdrücklich bestimmt ist, dass der Betroffene Bürger aus dem Rechtshilfeabkommen selbst keinerlei Rechte ableiten kann.

Damit bleibt dem deutschen Betroffenen auch hier nur der Weg, die einschlägigen deutschen Behörden mit Auskunftsverlangen und gegebenenfalls vorbeugenden Unterlassungsbegehren zu traktieren. Ist die Datenübertragung im Rechtshilfeweg bereits geschehen, kommt eine Klage auf Rückholung der Daten in Betracht, da die Einhaltung der deutschen Datenschutzbestimmungen durch das Rechtshilfeabkommen in keiner Weise gewährleistet ist.

Die Zweckbindungsbestimmungen des Rechtshilfevertrags, die nach Art. 1 VI keine individuellen Rechte begründen sollen, sind löchrig wie ein Schweizer Käse. Nach Art. 15 II dürfen die erlangten Informationen oder Beweismittel nicht zu einem anderen als dem in dem Ersuchen beschriebenen Zweck verwendet werden, „mit Ausnahme der in Absatz III aufgeführten Zwecke". Dort finden sich dann eine ganze Reihe von Ausnahmen, unter denen die Zweckbindung ohne vorherige Zustimmung des ersuchten Staates durchbrochen werden darf, nämlich

> „1. für jeden anderen Zweck, für den Rechtshilfe nach diesem Vertrag gewährt werden würde; 2. zur Verhinderung der Begehung schwerer Straftaten; 3. in einem nicht strafgerichtlichen Verfahren oder Verwaltungsverfahren, das sich auf einen in den Nummern 1. und 2. genannten Zweck bezieht und 4. zur Abwendung einer erheblichen Gefahr für die öffentliche Sicherheit."

Von dieser Ausnahme von der Zweckbindung gibt es eine weitere Ausnahme, dann nämlich, wenn der ersuchte Staat zum Zeitpunkt der Ablieferung der Daten ausdrücklich eine Zweckbindung verfügt. Wie diese Zweckbindung gewährleistet werden soll, sagt das Abkommen nicht. Lediglich für den Fall, dass ein Beweismittel oder eine Auskunft vorbehaltlich einer Bedingung zur Verfügung gestellt wird, kann der ersuchte Staat vom ersuchenden Staat verlangen, dass er die Verwendung der erhaltenen Informationen nachträglich darlegt. Welche Folgen es haben soll, wenn sich herausstellt, dass die erhaltenen Informationen bedingungswidrig verwandt wurden, sagt das Abkommen nicht.

Alle vier dargestellten Abkommen sind entweder direkte Folgen des 11. September 2001 oder jedenfalls in der Form, in der sie jetzt zustande gekommen sind, wesentlich durch die Ereignisse dieses Tages bestimmt. Gerade in dieser Situation hätte man vom „alten Europa" erwarten können, dass es seine Grundsätze energischer verteidigt.

Hartmut Wächtler ist Fachanwalt für Strafrecht in München.

War on Terrorism oder War on Liberty?

Schlechte Zeiten für die Bürgerrechte in den USA

von Clemens Arzt

„Es ist weder wünschenswert noch wahrscheinlich, dass Bürgerrechte in Kriegszeiten eine derart wichtige Rolle einnehmen, wie im Frieden.“[1] Diese Vorhersage des Vorsitzenden Richters am US-Supreme Court ist Realität geworden, seitdem die US-Regierung nach den Anschlägen vom 11. September 2001 den „war on terrorism“ ausgerufen hat.

Ihren Krieg gegen den Terror führen die USA auch nach innen. Allein im Jahr 2003 geben sie dafür rund 40 Mrd. Dollar aus. Seit dem Homeland Security Act vom 25.11.2002 werden neue organisatorische Strukturen für die Terrorismusbekämpfung, die Einwanderung und insbesondere das Department of Homeland Security geschaffen.

Das wohl wichtigste unter den neuen „Anti-Terror-Gesetzen“, der USA Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism – nachfolgend USAPA) vom 26.10.2001, brachte eine Vielzahl neuer Straftatbestände und Befugnisse. Der USAPA ist ein umfangreiches und unüberschaubares Artikelgesetz. Dieses führt zu einer deutlichen Gewichtsverschiebung von der Verfolgung von Straftaten unter der Prämisse der Unschuldsvermutung hin zu Maßnahmen zur (erhofften) Prävention terroristischer Akte und allgemeiner Straftaten unter häufig wenig bestimmten gesetzlichen Voraussetzungen. Das Gesetz erweitert zudem die Zulässigkeit des Einsatzes nachrichtendienstlicher Mittel und viele Tatbestände des materiellen Strafrechts, insbesondere den strafrechtlichen

1 Rehnquist, W.H.: All the Laws but One, New York 1998, p. 224

Terrorismusbegriff. Die Folge ist eine massive Beschränkung von Freiheitsrechten, wie nachfolgend dargestellt wird.

Maßnahmen, die darauf abzielen, Informationen über den Inhalt (content) menschlicher Kommunikation zu erlangen (intercept), sind in Abschnitt III des Omnibus Crime Control and Safe Streets Act von 1968 (Title III) geregelt. Der USAPA und später eingefügte Änderungen haben die Eingriffsvoraussetzungen für Abhörmaßnahmen wie auch den Zugang zu elektronisch gespeicherten Kommunikationsinhalten (z.B. voice mail) herabgesetzt.[2] Um eine möglichst weitgehende Verwendung der gewonnenen Informationen zu gewährleisten, wurde die bisher geltende strikte Abgrenzung von Strafverfolgungsbehörden und Nachrichtendiensten aufgeweicht. Zum Zwecke der Terrorabwehr können die Sicherheitsorgane nunmehr im Grunde unbeschränkt Informationen austauschen, die durch Abhörmaßnahmen gewonnen wurden.[3] Auch die Zulässigkeit des Einsatzes so genannter Pen-register- und Trap-and-trace-Maßnahmen wurde erweitert. Hierbei werden nach amerikanischem Verständnis nicht die Inhalte der Kommunikation erfasst, sondern nur Rufnummern und ähnliche Informationen. Die Novellierung erlaubt es, diese Überwachungsmethoden, die bislang vorwiegend für den Telefonverkehr Anwendung fanden, auch in Bezug auf den E-Mail-Verkehr und die Internetnutzung einzusetzen.[4] Eine Ausspähung des Inhalts der Kommunikation ist nach diesen Normen zwar weiterhin nicht zulässig.[5] Die Abgrenzung dessen, was als Inhalt anzusehen ist, scheitert indes häufig, weil beispielsweise die URL im Internetverkehr oder per Telefon übertragene Daten zur Verwaltung eines Bankkontos inhaltliche Informationen darstellen können.

Um eine vollständige Neuregelung handelt es sich bei den erstmals in das Gesetz aufgenommenen sneak and peek warrants. Danach sind heimliche Durchsuchungsmaßnahmen wie auch die verzögerte Bekanntgabe des Durchsuchungsbeschlusses zulässig, wenn der anordnende Richter der Auffassung ist, dass die Kenntnis der Maßnahme nachteilig für die Untersuchung sein könnte, weil Beweismittel zerstört werden

2 Public Law 107-56; vgl. insbesondere Title II USAPA, der die Vorschriften in 18 U.S.C.A. §§ 2510-2522 (= United States Code Annotated, vol. 18, sections 2510-2522) in vielfältiger Weise ändert.

3 18 U.S.C.A. § 2517(6)

4 18 U.S.C.A. § 3121(c)

5 18 U.S.C.A. § 3127(1) und (3)

könnten, Leib oder Leben einer Person gefährdet ist, bei Fluchtgefahr oder wenn sonst die Untersuchung erheblich gefährdet oder das Verfahren ungebührlich verzögert werden könnten.[6] Die Benachrichtigung hat in angemessener Zeit nach der Vollziehung zu erfolgen, wobei die vom Richter zu bestimmende Zeitdauer verlängert werden kann, wenn hierfür ein guter Grund vorliegt.[7] Im Rahmen einer solchen Durchsuchung dürfen im Regelfall keine beweglichen Gegenstände beschlagnahmt werden, sofern der anordnende Richter hierfür nicht eine berechtigte Notwendigkeit erkennt.[8]

Foreign Intelligence Surveillance Act (FISA)

Die Praktiken insbesondere der Nixon-Regierung und die Überwachung politischer Gegner im Innern seitens der Geheimdienste gaben 1978 den Anstoß zur Schaffung des Foreign Intelligence Surveillance Act (FISA).[9] Aufgaben und Zuständigkeiten der Strafverfolgung wurden klar von denen der Behörden zur Aufrechterhaltung der nationalen Sicherheit getrennt. Die Zuständigkeit der Nachrichtendienste im Innern des Landes wurden beschränkt, die Zuständigkeit der Terrorismusbekämpfung vorrangig dem FBI übertragen.

FISA soll heute die nachrichtendienstliche Tätigkeit zum Zwecke der Abwehr feindlicher Bestrebungen ausländischer Staaten und Organisationen, von Terroristen und ihren Helfern in den USA regeln.[10] Das Gesetz statuiert die Anforderungen für ein von der Strafverfolgung grundsätzlich getrenntes, mit den dort bekannten Maßnahmen aber mittlerweile im Wesentlichen identisches Bündel von Eingriffsbefugnissen. Maßnahmen sind zulässig, wenn hinreichender Grund zu der Annahme besteht, dass sich die Maßnahme gegen eine ausländische Macht oder deren Agenten richtet.[11] Ist die Zielperson US-Staatsbürger oder verfügt sie über einen dauerhaften Aufenthaltsstatus, gelten gewisse Einschränkungen.[12] Da das Gesetz nicht den Verdacht oder das Bevorstehen einer Straftat fordert, ermöglicht es wesentlich früher einsetzende und weiter-

6 18 U.S.C.A. 3103a(b)
7 18 U.S.C.A. 3103a(b)(3)
8 18 U.S.C.A. 3103a(b)(2)
9 50 U.S.C. §§ 1801-1862
10 50 U.S.C.A. § 1801(e)
11 50 U.S.C.A. § 1805(a)(3)(A)
12 vgl. 50 U.S.C.A. §§ 1805(a)(3)(A) und 1842(a)(1); §§ 1801(h), 1805(a)(4); 1824(a)(4)

gehende Überwachungsmaßnahmen als dies strafprozessual der Fall wäre. Mit Blick auf die niedrige Eingriffsschwelle ist die Verwendung von Beweismitteln aus einer Maßnahme nach FISA im Strafverfahren verfassungsrechtlich problematisch, wird aber in der Regel von den Gerichten nicht beanstandet.

Die Anordnungsbefugnis für Maßnahmen nach FISA liegt bei einem 1978 eigens geschaffenen Geheimgericht, dem Foreign Intelligence and Surveillance Court (FISC), dessen Entscheidungen vom Foreign Intelligence and Surveillance Court of Review (FISCR) überprüft werden können. Gerichtsbeschlüsse über die Zulässigkeit von Überwachungsmaßnahmen (warrant) sind den Betroffenen gegenüber geheim und können daher im Regelfall nicht gerichtlich überprüft werden, solange die gewonnenen Erkenntnisse nicht in einem Strafverfahren oder anderen Verfahren verwendet werden sollen.[13] Im Notstandsfalle kann der Attorney General die angeführten Maßnahmen ohne richterliche Entscheidung autorisieren, muss aber eine nachträgliche richterliche Entscheidung einholen.[14] Zwischen 1978 und 2001 gab es 47 solcher emergency-Anordnungen, in den ersten 12 Monaten nach dem 11. September 113.[15]

Durch den USA Patriot Act wurden die behördlichen Befugnisse im Rahmen der durch FISA vorgesehenen Maßnahmen ausgeweitet. Die maximale Geltungsdauer von Abhörmaßnahmen und Durchsuchungsbeschlüssen wurde auf bis zu 365 Tage verdoppelt. Zukünftig sind Maßnahmen nach FISA nicht mehr vorrangig (primary purpose) auf die Abwehr von foreign intelligence beschränkt, sondern es genügt, wenn diese ein wesentliches Ziel (significant purpose) der Maßnahme ist.[16] Unter foreign intelligence fallen unter anderem Informationen, die sich auf potentielle Angriffe ausländischer Mächte oder ihrer Handlanger oder auf den internationalen Terrorismus beziehen.[17] Um eine Maßnahme der Strafverfolgung auf FISA zu stützen, reicht es mithin aus, wenn diese zugleich für nachrichtendienstliche Zwecke bedeutsam ist. Dies führt zu einer weiteren Verwischung der Grenzen von Strafverfahren und nachrichtendienstlichen Maßnahmen. Die Gefahr, dass auch Strafverfol-

13 50 U.S.C.A. § 1806(c)
14 50 U.S.C.A. §§ 1805(f), 1824(e), 1843
15 Department of Justice (DOJ): ohne Titel (Stellungnahme zum USAPA), 13.5.2003, www.house.gov/judiciary/patriotlet 051303.pdf, Ziff. 14
16 50 U.S.C.A. §§ 1804(a)(7)(B) und 1823(a)(7)(B)
17 50 U.S.C.A. § 1801(e)

gungsbehörden vermehrt quasi geheimdienstliche Methoden anwenden, wächst.

Nach neuer Rechtslage können alle Kommunikationsverbindungen des Betroffenen überwacht werden, unabhängig vom Ort, an dem die Kommunikation stattfindet. Die Eingriffe in die Privatsphäre gehen erheblich weiter als nach altem Recht, weil sich die Maßnahme nunmehr auch gegen öffentlich zugängliche Einrichtungen richten können: Die Behörde kann z.B. ein Internet-Café oder eine öffentliche Bibliothek mit Internetzugang überwachen, wenn sie annimmt, dass die Zielperson diese für Kommunikationszwecke nutzen könnte.[18] Erweitert wurden auch die subpoena-Befugnisse des FBI: Auf der Basis eines Gerichtsbeschlusses kann das FBI jede natürliche oder juristische Person zur Herausgabe jedweder beweglichen Sache zwingen. Voraussetzung ist, dass die Untersuchung den Schutz gegen den internationalen Terrorismus oder geheime nachrichtendienstliche Aktivitäten bezweckt und sich nicht ausschließlich auf Tätigkeiten bezieht, die unter den Schutz des ersten Verfassungszusatzes (Meinungsfreiheit) fallen.[19] Dass eine solche Herausgabe verlangt oder Unterlagen herausgegeben wurden, darf der Betroffene Dritten oder der Presse nicht offenbaren.[20] Eine vergleichbare Maßnahme stellen auch die so genannten national security letters dar, die die Betroffenen verpflichten, bestimmte elektronisch aufgezeichnete Daten (Finanzdaten, Telefon- und E-Mail-Daten etc.) aus nachrichtendienstlichen Gründen an die Behörden herauszugeben.[21]

Maßnahmen gegen Ausländer und Immigranten

Nach einer neu geschaffenen Bestimmung im Immigration and Nationality Act muss (!) der Attorney General jeden Ausländer in Gewahrsam (mandatory detention) nehmen, von dem er aus „berechtigten Gründen" annimmt, dass dieser die nationale Sicherheit gefährdet.[22] Wird innerhalb von sieben Tagen kein Abschiebe- oder Strafverfahren eröffnet, ist der Betroffene grundsätzlich freizulassen. Der Attorney General kann jedoch (wiederholt) für maximal sechs Monate eine Fortdauer des Ge-

18 ebd.
19 50 U.S.C.A. §§ 1861(a)(1)
20 50 U.S.C.A. §§ 1861(d)
21 vgl. DOJ a.a.O. (Fn. 15), Ziff. 3 m.w.N.
22 8 U.S.C.A. § 1226a

wahrsams anordnen, soweit die Freilassung eine Gefahr für die nationale Sicherheit der USA oder die Sicherheit des Gemeinwesens oder für irgendeine Person darstellt. Eine gerichtliche Überprüfung ist nur im Rahmen eines Habeas-Corpus-Verfahrens möglich, bei dem erst nach Gewahrsamnahme über deren Zulässigkeit entschieden wird.

Unter Rückgriff auf ausländerrechtliche Bestimmungen wurden in den ersten Monaten nach dem 11. September mehr als 1.200 Ausländer als Terrorismusverdächtige in Gewahrsam genommen, rund 750 wurden für längere Zeit festgehalten. Rund 50 Personen werden oder wurden als wichtige Zeugen (material witness) festgehalten, obgleich ihnen selbst kein Vorwurf gemacht wird.[23] Rechtsverletzungen und physische wie psychische Misshandlungen waren nach mittlerweile offizieller Bekundung keine Ausnahme.[24] Mitte 2003 begann eine Kampagne, bei der rund 13.000 Männer aus 25 arabischen und/oder muslimischen Ländern wegen der Verletzung aufenthaltsrechtlicher Vorschriften abgeschoben werden sollen. Der Abschiebung ging eine Anordnung voraus, nach der sich alle Männer aus diesen Ländern bei den Behörden melden mussten, wovon rund 82.000 Menschen erfasst waren.

Eine Änderung des International Emergency Economic Powers Act (IEEPA) von 1977 ermöglicht es, ohne rechtsstaatliches Verfahren Eigentum und Vermögen ausländischer Staaten, Organisationen oder Personen zu sperren und Geschäfte mit ihnen zu untersagen.[25] Anordnen kann dies der Präsident u.a. im Falle eines Angriffs aus dem Ausland, wenn die Betroffenen nach seiner Einschätzung Feindseligkeiten oder Anschläge gegen die USA geplant, autorisiert, unterstützt oder ausgeführt haben.[26] Nach dem 11. September wurden die Guthaben verschiedener muslimischer Gruppierungen eingefroren. Insgesamt waren hiervon bis zum Frühjahr 2003 etwa 600 Bankkonten mit einem Gesamtguthaben von rund 124 Mio. Dollar betroffen.[27]

---

23 anschaulich United States v. Awadallah, 202 F.Supp.2d 55 und 82 (= Federal Supplement, vol. 202, second series, pp. 55, 82) sowie In Re Application Of U.S. For Material Witness Warrant, 213 F.Supp.2d 287

24 vgl. den Bericht des Inspector General beim Justizministerium, www.usdoj.gov/oig/special/03-06/index.htm

25 50 U.S.C.A. §§ 1701-1707

26 vgl. Executive Order 13224, 66 Fed. Reg. (=Federal Register) S. 49079 v. 25.9.2001 sowie die Änderungen durch Executive Order 13268, 67 Fed. Reg. S. 44751 v. 3.7.2002

27 Global Relief Foundation v. O'Neill, 207 F.Supp.2d 779, 315 F.3d 748; Holy Land Found For Relief and Development v. Ashcroft, 219 F.Supp.2d 57; DOJ a.a.O. (Fn. 15), Ziff. 17.A

Einrichtung von Militärtribunalen

Die geplante Anklage von Terrorismusverdächtigen und anderen Personen vor Militärtribunalen basiert auf einer Anordnung des Präsidenten vom 13.11.2001. Unter deren Anwendungsbereich fallen insbesondere die rund 650 in Guantanamo und an geheimen Orten festgehaltenen Personen. Auch US-Staatsbürger können dem „normalen" Strafprozess dadurch entzogen werden, dass der Präsident sie zu feindlichen Kombattanten erklärt.[28] Dies kann der Betroffene allenfalls dadurch vermeiden, dass er in eine Absprache (plea bargaining) einwilligt, d.h. sich schuldig erklärt und auf ein ordentliches Strafverfahren verzichtet.[29] Voraussichtlich im Jahr 2004 wird sich der US Supreme Court erstmals mit der Rechtmäßigkeit dieser Maßnahmen befassen.[30] In den Militärtribunalen werden Militärs in einem rechtsstaatlichen Grundsätzen nicht entsprechenden Verfahren über das Schicksal der Betroffenen entscheiden. Angeklagt werden kann jede Person, von der der Präsident Grund zu der Annahme hat, dass sie den internationalen Terrorismus unterstützt oder hieran beteiligt ist.[31] Entscheidungen dieser Tribunale sollen vor ordentlichen Gerichten und Kriegsgerichten der USA, ausländischen (!) und internationalen Gerichten nicht anfechtbar sein.[32] In der Exekutive besteht allerdings noch Uneinigkeit darüber, ob auch eine Überprüfung im Rahmen einer Habeas-Corpus-Anfechtung ausgeschlossen sein soll. Auch wenn das Militärtribunal zu dem Ergebnis gelangt, dass einer Person nichts vorzuwerfen sei, hat sie keinen Anspruch auf Freilassung. Über die Fortdauer des Gewahrsams entscheidet allein die Exekutive.

Gezielte Tötungen

In der deutschen Öffentlichkeit bislang wenig Beachtung gefunden haben Diskussionen zu gezielten Tötungen oder Ermordungen politischer Gegner außerhalb des Territoriums der USA. Section 2.11 der Executive Order No. 12333 des Präsidenten vom 4.12.1981 verbietet Morde durch

28 vgl. Washington Post v. 30.7.2003
29 vgl. Washington Post v. 29.7.2003
30 vgl. Hamdi v. Rumsfeld (03-6696); M.K.B. v. Warden (03-6747); Rasul v. Bush (03-334); Al Odah v. U.S. (03-343)
31 Anordnung vom 13.11.2001, Sec. 2(a)(1) (=66 Fed. Reg. S. 57833 v. 16.11.2001)
32 ebd., Sec. 7(b)(2)

Regierungsmitarbeiter oder -beauftragte.[33] Allerdings hat der Kongress am 18.9.2001 eine Joint Resolution beschlossen, welche auch den Einsatz von Gewalt (all necessary and appropriate force) legitimiert.[34] Juristen, die der Exekutive möglichst wenig Beschränkungen auferlegen wollen, vertreten, dass diese Entschließung auch gezielte Tötungen politischer Gegner legitimiere und der Executive Order No. 12333 vorgehe, soweit es sich dabei um Akte der Selbstverteidigung handele.

Fazit

Der War on Terrorism droht selbst nach Einschätzung konservativer Kritiker zu einem War on Liberty zu werden, für viele Betroffene hat er diese Dimension bereits angenommen.[35] So wurden die neuen Strafnormen und Eingriffsbefugnisse zum Beispiel gegen einen Drogenhändler, einen vierfachen Mörder, eine „liebeskranke“ Zwanzigjährige und andere Personen angewandt, die keineswegs unter Terrorismusverdacht standen.[36] Opfer der so genannten Anti-Terror-Maßnahmen sind zumeist Ausländer oder Immigranten. Zwar gibt es eine erstarkende Gegenbewegung und einige der gesetzlichen Neuregelungen sollen Ende 2005 außer Kraft treten. Der mit dem War on Drugs eingeläutete und mit dem War on Terrorism konsequent fortgesetzte Abbau von Freiheitsrechten wird möglicherweise auch hier und da korrigiert werden; die bürgerrechtliche Aufbruchstimmung der sechziger und frühen siebziger Jahre dürfte jedoch so schnell nicht wiederkehren.

Clemens Arzt ist Professor an der Fachhochschule für Verwaltung und Rechtspflege Berlin (FHVR).

33 46 Fed. Reg. S. 59941 v. 8.12.1981

34 Public Law 107-40

35 vgl. Gingrich, N.: The Politics of War – Refocus the Mission, in: San Francisco Chronicle v. 11.11.2003

36 Vgl. New York Times v. 28.9.2003; DOJ a.a.O. (Fn. 15), Ziff. 16, wo detailliert die Nutzung der neuen Befugnisse dargestellt wird.

Die Wissenschaft hat festgestellt ...

Die Verharmlosung der Telekommunikationsüberwachung

von Norbert Pütter

Am 15. Mai 2003 präsentierte Bundesjustizministerin Brigitte Zypries das im Auftrag ihres Ministeriums erstellte Gutachten des Max-Planck-Instituts für ausländisches und internationales Strafrecht (MPI) über die Telekommunikationsüberwachung (TKÜ) in der Bundesrepublik.[1] Die Untersuchung zeige, so Zypries, dass die TKÜ „ein unverzichtbares und effizientes Mittel zur Strafverfolgung" sei, das „von den Ermittlungsbehörden sensibel und unter Wahrung des Verhältnismäßigkeitsgrundsatzes eingesetzt" werde.[2]

Die Vorgeschichte des Gutachtens geht auf die erste rot-grüne Koalitionsvereinbarung von 1998 zurück. Unmittelbarer Anlass war die in den 1990er Jahren explosionsartig gestiegene Zahl der Telefon- bzw. Telekommunikationsüberwachungen. Das Gutachten sollte Licht in das Dunkel der Überwachungspraxis bringen und damit die Grundlage für eventuelle Reaktionen des Gesetzgebers bilden. Da die Justiz- und Innenverwaltungen seit Jahrzehnten damit beschäftigt sind, selbst banale Statistiken der Öffentlichkeit vorzuenthalten, war die Idee eines wissenschaftlichen Gutachtens durchaus sachlich begründet. Allerdings hatte sie auch damals schon die Funktion, die eigentlich nicht erwünschte Novellierung

1 Mittlerweile auch als Buch: Albrecht, H.-J.; Dorsch, C.; Krüpe, C.: Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen, Freiburg 2003. Die Seitenangaben im Text beziehen sich auf das Gutachten. Dieses ist auch im Volltext auf der Homepage des Max-Planck-Instituts zugänglich: www.iuscrim.mpg.de/verlag/online/Band_115.pdf.

2 Bundesministerium der Justiz, Zypries: Telefonüberwachung wirksam und maßvoll, Pressemitteilung v. 15.5.2003

auf die lange Bank einer wissenschaftlichen Expertise zu schieben. Während das MPI forschte und sich die Fertigstellung des Gutachtens mehrfach verzögerte, wurde der Katalog der Straftaten, die eine TKÜ erlauben, mehrfach erweitert: direkt durch die Aufnahme des schweren sexuellen Missbrauchs von Kindern und die Verbreitung pornografischer Schriften,[3] indirekt durch die Einführung des § 129b (kriminelle und terroristische Vereinigung im Ausland) ins Strafgesetzbuch.[4] Parallel hierzu wurden KritikerInnen, die eine restriktivere Fassung der TKÜ-Bestimmungen wollten, mit dem Hinweis auf das ausstehende Gutachten auf die Zukunft vertröstet.[5]

Die Untersuchung

Das MPI nutzte die Gelegenheit des Gutachtens zu einer aufwändigen Untersuchung, die nicht nur für Deutschland Neuland betritt, sondern auch im weltweiten Vergleich (fast) einzigartig ist. Um „Rechtwirklichkeit und Effizienz" der TKÜ zu erfassen, wählte das Institut einen Zugang über drei verschiedene Methoden:

Erstens wurden die Akten von Strafverfahren analysiert, in denen es zu einer TKÜ gekommen war. Da die Verfahren abgeschlossen und die Unterlagen zugänglich sein sollten, wurden die Verfahren aus dem Jahr 1998 für die Untersuchung genutzt. Nach der Statistik der Länder waren in diesem Jahr 2.705 Verfahren mit TKÜ-Maßnahmen gemeldet worden. Durch eine gewichtete Zufallsstichprobe wurden 813 Verfahren für die Analyse ausgewählt. Bis zum Ende der Auswertungen wurden dem MPI jedoch nur die Akten von 523 Strafverfahren zur Verfügung gestellt (S. 133f.). Die Aktenanalyse ergab, dass es in 22 Fällen zu keiner TKÜ gekommen war, so dass für die Untersuchung 501 Verfahren ausgewertet werden konnten. In diesen Verfahren kam es zu 1.700 TKÜ-Anordnungen, die 2.783 Anschlüsse betrafen (S. 147).[6]

Zweitens wurden Einschätzungen und Meinungen über die TKÜ in einer schriftlichen Befragung erhoben. Insgesamt versandte das MPI 6.256 Fragebögen an Beschäftigte bei Polizeien, Staatsanwaltschaften,

3 BGBl. I v. 10.10.2002, S. 3954
4 BGBl. I v. 22.8.2003, S. 3390
5 BT-Drs. 15/725 v. 28.3.2003
6 Laut TK-Regulierungsbehörde ergingen bundesweit 1998 9.802 TKÜ-Anordnungen (S. 30), demnach umfasst die MPI-Stichprobe ca. 17,3 % der Überwachungen von 1998.

Gerichten sowie an StrafverteidigerInnen. Die Rücklaufquote betrug insgesamt 46 %; am höchsten war sie bei den PolizistInnen (77 %), bei den anderen drei Gruppen lag sie zwischen 33 und 36 % (S. 140).

Um Detailwissen und praktische Erfahrungen in die Untersuchung einbringen zu können, wurden drittens 43 Personen anhand eines Fragenkatalogs (meist telefonisch) interviewt. Auch diese Experten entstammten den genannten vier Berufsgruppen (S. 141).

Die Untersuchung erweitert das bisherige Halbwissen über die TKÜ erheblich. Sie bestätigt, dass der weit überwiegende Teil der TKÜ in den Ermittlungen wegen Rauschgiftkriminalität stattfindet (199 der 501 Verfahren); weit abgeschlagen folgen Raub- und Mordermittlungen mit 55 bzw. 46 Verfahren (S. 145). Die Studie bestätigt weiter, dass in der zweiten Hälfte der 90er Jahre Mobiltelefon-Anschlüsse fast die Hälfte aller überwachten Anschlüsse ausmachten (S. 150). Das Gutachten enthält detaillierte Angaben über die Zahl der Beschlüsse und die Anzahl der überwachten Anschlüsse pro Verfahren, über das Alter der Beschuldigten und deren Verteilung auf die Verfahren. Darüber hinaus wird das „Schicksal“ der TKÜ im Verlauf des Ermittlungsverfahrens dargestellt – beginnend mit den Informationsquellen, die die Verfahren mit TKÜs in Gang setzten, über den Zeitpunkt, ab dem es zur Überwachung kam, bis zur Bedeutung der TKÜ-Ergebnisse im Strafprozess. Interessant sind auch die Angaben über die Zahl der abgehörten Gespräche pro Anordnung bzw. Verfahren (Spannweite zwischen 0 und 30.500 Gesprächen). Auch wenn die Akten fünf Jahre alte Vorgänge betreffen, so kann nun niemand mehr behaupten, über die TKÜ sei kaum etwas bekannt. In dieser Hinsicht wären vergleichbare Untersuchungen für die anderen geheimen Ermittlungs- und Polizeimethoden sehr wünschenswert.

Wald und Bäume

Die Detailfülle, mit der der Bericht auf 472 Seiten aufwartet, verdeckt jedoch, dass das MPI die ihm gebotenen Chancen nicht genutzt hat. Zunächst fällt auf, dass der Bericht mit wenig relevanten Informationen aufgebläht ist. Warum etwa die rechtlichen TKÜ-Regelungen in Schottland oder Neuseeland dargestellt werden, bleibt unverständlich. Auch auf das Recht der vierzehn weiteren vorgestellten Länder wird in anderen Teilen der Untersuchung nur vereinzelt Bezug genommen. Interessante Fakten ausländischer Vorschriften sind dagegen nur am Rande erwähnt und in ihrer praktischen Bedeutung allenfalls in Ansätzen erfasst, so etwa

das Minimierungsgebot (S. 95) und die „consent surveillance“ (S. 124) in den USA. Eine solch oberflächliche Darstellung ergibt keine Anregungen für die deutsche Diskussion.

Nachteilig auf den Ertrag der Studie wirkt sich auch aus, dass die AutorInnen offenkundig unter Evaluation nur etwas verstehen, was in Zahlen ausgedrückt werden kann. Ansonsten ist nicht erklärlich, warum einige einschlägige Untersuchungen zu den verdeckten Methoden von ihnen nicht zur Kenntnis genommen wurden.[7] Dass sie die Monografie von Zimmermann nicht erwähnen, ist darüber hinaus ein Indiz, dass sie an der rechtspolitischen Funktion der Telefonüberwachung nicht interessiert sind.[8] Wichtiger als diese Kleinigkeiten, die eher das Umfeld des Gutachtens betreffen, ist der Umstand, dass die Kriterien, an denen Rechtswirklichkeit und Effizienz gemessen werden, im Laufe der Untersuchung immer undeutlicher werden. Je differenzierter die Operationalisierungen und Auszählungen, desto fragwürdiger werden die Befunde und die Schlussfolgerungen, die das Gutachten selbst zieht und damit der Ministerin und anderen politisch Verantwortlichen in den Mund legt. An vier Komplexen soll dies im Folgenden kurz dargestellt werden: dem Anstieg der Überwachungen in den 90ern, der Stellung der TKÜ im Ermittlungsverfahren, der Bedeutung von Anordnungs- und Benachrichtigungspflichten und dem Ertrag der Überwachungen.

Der TKÜ-Boom

Vor der Auswertung des selbst erhobenen Materials setzt sich die Studie mit dem Anstieg der TKÜ in den 90er Jahren auseinander. Von 1995 bis 1998 stieg die Zahl von 3.667 auf 9.802 Anordnungen, im Jahr 2000 betrug sie bereits 15.741 und – eine Zahl, die der Bericht nicht mehr enthält – bis 2002 war sie auf 21.974 gestiegen. Die Untersuchung prüft einige Erklärungen für diese dauerhaften Steigerungen. Dass der Anstieg eine Folge gestiegener Kriminalität sei, wird überzeugend zurückgewiesen. Vielmehr würde mehr überwacht, weil es mehr Mobiltelefone gebe. Dies zeigten auch die nach Anschlussarten aufgeschlüsselten Anordnungen: die Festnetzzahlen blieben fast stabil, während das Wachstum allein

7 z.B.: Stock, J.; Kreutzer, A.: Drogen und Polizei, Bonn 1996, S. 284 ff.; Pütter, N.: Der OK-Komplex, Münster 1998, S. 180 ff.; Busch, H.: Polizeiliche Drogenbekämpfung – eine internationale Verstrickung, Münster 1999, S. 238 ff.

8 Zimmermann, G.: Staatliches Abhören, Frankfurt a.M. u.a. 2001

auf Mobilfunkanschlüsse zurückzuführen sei (S. 36f.). Im Kontext der Untersuchung ist diese Feststellung allerdings wenig hilfreich. Zum einen kann die gewählte Erklärung nicht beantworten, warum die TKÜs seit ihrer Legalisierung 1968 permanent zunahmen: etwa von 1980 bis 1986 um 100 %.[9] Sollte es noch andere Gründe für den Anstieg geben? Auch der internationale Vergleich wäre in dieser Hinsicht aufschlussreich. Das MPI führt ihn an, um zu belegen, dass Deutschland nicht „Überwachungs-Weltmeister" ist. Aber hat die Mobiltelefonie in den 90ern nicht auch in den USA, Frankreich und Österreich zugenommen? Mit anderen Worten: Es gibt keinen Automatismus zwischen Mobilfunkrate und Überwachung. Warum hat das MPI z.B. nicht erhoben, welche Polizeidienststellen die TKÜs beantragen? Dann hätte man zumindest die Vermutung prüfen können, dass bestimmte Polizeistrategien für das Überwachungs-Wachstum verantwortlich sind. Immerhin haben über 58 % aller TKÜ-Verfahren ihren Ursprung in anderen polizeilichen Ermittlungen (davon über 14 % in anderen TKÜs, S. 154). Warum verliert das Gutachten kein Wort darüber, dass die enormen Steigerungen nur möglich sind, wenn die entsprechende Technik bei der Polizei angeschafft wird, und dass deren Anschaffung auf bewusste Entscheidungen zurückgeht?[10] Warum fragt das MPI nicht nach den Gründen für die unterschiedliche TKÜ-Überwachungsdichte in den Bundesländern?[11] Die Oberflächlichkeit des Gutachtens wird in dieser Hinsicht gekrönt durch den Vergleich von TKÜ- und Mobiltelefonie-Steigerungen. Da die TKÜs langsamer zugenommen hätten als die Handys, sei die Überwachungsdichte sogar zurückgegangen (S. 38)! Bisher ging man in demokratischen Rechtsstaaten davon aus, dass ein Grundrechtseingriff nicht davon abhängt, wie oft jemand redet oder telefoniert, sondern ob er oder sie einer bestimmten Tat verdächtig ist. Worin bestünde ansonsten der Unterschied zum Überwachungsstaat?!

Vom letzten zum ersten Mittel

9 Pütter, N.: Fernmeldeüberwachung, in: Bürgerrechte & Polizei/CILIP 60 (2/1998), S. 36-42 (41f.)

10 Bizer, J.: Die Evaluierung der Telekommunikations-Überwachung. Anmerkungen zur MPI-Studie, in: Kriminologisches Journal 2003, H. 4 (im Erscheinen)

11 ebd.

Seit 1968 ist die Telefon- bzw. die Telekommunikationsüberwachung in den §§ 100a und 100b der Strafprozessordnung (StPO) geregelt. Dem damaligen Gesetzgeber war bewusst, dass es sich um einen Eingriff in ein wichtiges Grundrecht handelte. Deshalb wurde die Telefonüberwachung an eine Reihe von Bedingungen gebunden: Zulässigkeit nur bei bestimmten Taten (der Katalog wurde bekanntlich ständig erweitert), Anordnung durch den Richter (allein bei Gefahr im Verzuge durch die Staatsanwaltschaft), die nachträgliche Benachrichtigung der Betroffenen und durch die Subsidiarität der Maßnahme, d.h. sie darf nur dann eingesetzt werden, wenn die Ziele (Aufklärung des Sachverhalts, Aufenthaltsermittlung des Tatverdächtigen) „auf andere Weise aussichtslos oder wesentlich erschwert wäre".[12]

Durch spätere Novellierungen der StPO wurden andere verdeckte Methoden ebenfalls an Subsidiaritätsklauseln gebunden; etwa der Einsatz Verdeckter Ermittler oder die Überwachung mit technischen Mitteln. Unabhängig von der Frage, welches der „letzten Mitteln" zuerst eingesetzt werden soll, besagt die Subsidiaritätsklausel, dass zunächst weniger in die Rechte der Beschuldigen eingreifende Maßnahmen ergriffen werden müssen, dazu zählen z.B. Zeugenbefragungen, Vernehmungen oder Durchsuchungen.

Die MPI-Studie zeigt, dass von Subsidiarität beim TKÜ-Einsatz nicht die Rede sein kann. Statt „Ultima Ratio" habe die Überwachung der Telekommunikation „die Funktion eines Mittels der ersten Wahl" (S. 159). Auch ein Vergleich unterschiedlicher Verfahrensgruppen zeigt, dass im Hinblick auf organisierte und „marktförmige Kriminalität" entgegen den Vorgaben des Gesetzgebers die verdeckten Methoden nicht am Ende, sondern am Anfang polizeilicher Ermittlungen stehen (S. 304). Handelt es sich hingegen um Delikte der „klassischen" Kriminalität, wie Mord und Raub – denen nur ein kleiner Teil der TKÜs gelten –, dann beginnen die Ermittlungen mit offenen Maßnahmen (S. 313).

Das Gutachten sieht in dieser Umkehrung des Rechts durch die Praxis eine unmittelbare Folge der Kriminalitätsentwicklung. Fehlende Opfer, Abschottung, dauerhafte illegale Marktbeziehungen erlaubten keinen anderen Zugang als den über verdeckte Methoden. In seinen abschlie-

12 Die Auskunftsersuchen nach § 12 des Fernmeldeanlagengesetzes (nicht über den Inhalt, sondern die Umstände der Kommunikation (= Verbindungsdaten, Dauer etc.)) spielten 1998 quantitativ eine geringe Rolle. Sie werden im Folgenden nicht gesondert betrachtet. Die Bestimmung wurde 2001 durch die §§ 100g und 100h der StPO ersetzt.

ßenden Empfehlungen regt das MPI denn auch an, für bestimmte Kriminalitätsformen eine „Sonderbetrachtung“ in die StPO einzuführen (S. 465f.). Bereits hier fällt auf, dass das Gutachten nichts über die Schwere oder Schädlichkeit jener Kriminalitätsformen aussagt, für die ein Sonder-Eingriffsrecht geschaffen werden soll. Offenkundig geht es dem Gutachten nur darum, das Recht der gängigen Praxis anzupassen.

Notare statt Kontrolleure

Das Grundrecht soll in der Logik der StPO nicht allein durch materielle Bestimmungen, sondern auch durch Vorschriften geschützt werden, die das Verfahren der TKÜ-Anordnung betreffen. § 100b StPO bestimmt, dass die TKÜ nur durch den Richter angeordnet werden darf; bei Gefahr im Verzuge kann sie für die Dauer von drei Tagen auch von der Staatsanwaltschaft angeordnet werden. Das MPI-Gutachten bestätigt, dass die staatsanwaltschaftlichen Eilanordnungen eine untergeordnete Rolle spielen (Anteil: 12 %, S. 175); es bestätigt auch, dass die Überwachungsanträge von Richtern so gut wie nie abgelehnt werden (0,4 %, S. 177). Sehr ausführlich prüft das Gutachten die Inhalte der Anträge und der richterlichen Überwachungsbeschlüsse.[13] Dies geschieht in expliziter Auseinandersetzung mit der im Dezember 2002 bekannt gewordenen Untersuchung von Backes und Gusy, die „den richterlichen Verzicht auf eine eigenständige Kontrolle staatsanwaltschaftlicher Anträge“ diagnostizierten und kritisierten.[14]

Das Gutachten untersucht die Begründungen für TKÜs auf drei Ebenen: bei Polizei, Staatsanwaltschaft und Gericht. Der Anteil der als „substantiell“ gewerteten Begründungen lag zwischen 28,5 (Polizei) und 23,5 % (Richter). Lediglich formelhafte Begründungen weisen zwischen

13 Bizer a.a.O. (Fn. 10) sieht im Zustand der Akten eines „der erschütternsten Ergebnisse der Untersuchung“. So konnte die Studie in der Hälfte der Fälle Antrags- und Anordnungstext nicht vergleichen, weil die Akten lückenhaft waren. Die schlampige Aktenführung, vom Gutachten mit keinem Wort gewürdigt, verletzt – so Bizer – die vom Grundgesetz geforderte Gesetzmäßigkeit der Verwaltung.

14 Backes, O.; Gusy, C.: Wer kontrolliert die Telefonüberwachung? Eine empirische Untersuchung von Richtervorbehalten bei Telefonüberwachungen, in: Strafverteidiger 2003, H. 4, S. 249-252. Mittlerweile als Buch veröffentlicht: Backes, O.; Gusy, C.: Wer kontrolliert die Telefonüberwachung?, Frankfurt u.a. 2003. Bemerkenswert ist, dass das MPI auch die Interviewpartner nach ihrer Bewertung der Studie befragt. Sie war zu diesem Zeitpunkt nur in einer knappen Zusammenfassung bekannt; selbst zum Zeitpunkt der Fertigstellung des Gutachtens war sie noch nicht veröffentlicht.

44,4 und 57,2 % der Anordnungen auf (S. 227-231). Zusammenfassend stellt das MPI fest, dass die Qualität der richterlichen Begründungen von den Anträgen der Polizei und der Staatsanwaltschaft abhängt (S. 235). Mit anderen Worten: Die Stichhaltigkeit einer TKÜ-Anordnung wird von Polizei und Staatsanwaltschaft vorgegeben und von Richtern im Regelfall „abgesegnet". Zur Erklärung verweisen Ermittlungsrichter in den Interviews auf ihre Arbeitslast. Ein Richter gibt an, er habe 10 bis maximal 30 Minuten Zeit für eine Entscheidung. Zusammen mit einem Kollegen müsse er pro Jahr 6.200 Entscheidungen bewältigen – darunter eben auch TKÜ-Anordnungen (S. 258). Dass die Richter sich unter diesen Bedingungen an die Formulierungen der Antragsteller halten, ist nachvollziehbar.

Das Gutachten diagnostiziert eine Diskrepanz zwischen Norm und Wirklichkeit. Wer an wen angenähert werden soll, lässt der Text zwar offen, aber die Sympathie gilt dem „kooperativ funktionierenden System", das auf „Vertrauen" und auf der Sach- und Fachkunde von PolizistInnen und StaatsanwältInnen aufbaue. Diese „Vertrauensbasis" sollte „gestärkt werden" (S. 268). Wie der Grundrechtsschutz, so scheint für das MPI auch die Gewaltenteilung ein antiquiertes Relikt vergangener Zeiten zu sein.

Niemanden beunruhigen

Sollte ursprünglich der Richtervorbehalt eine juristische Vorabkontrolle gewährleisten, so sollte die Benachrichtigungspflicht die von der TKÜ Betroffenen in die Lage versetzen, zumindest nachträglich die Rechtmäßigkeit ihrer Überwachung gerichtlich überprüfen zu lassen. Nur in Ausnahmefällen erlaubt § 101 StPO, dass die Betroffenen nicht informiert werden. Diese Ausnahme ist in der Praxis offenkundig die Regel. Die Aktenauswertung des MPI ergab, dass bei 6,4 % der überwachten Anschlüsse unter Bezug auf die Ausnahmeregelung die Benachrichtigung der Überwachten unterblieb. Direkte Benachrichtigungen erfolgten bei 15,3 % der Anschlüsse, indirekt (etwa über die Verteidigung oder das Strafverfahren) wurden die Betroffenen von weiteren 11,7 % informiert – dabei werden als Betroffene in der Regel nur die Anschlussinhaber verstanden. Für zwei Drittel aller Überwachungen konnte das MPI keinerlei Hinweise auf eine nachträgliche Benachrichtigung finden (S. 276).

Im Hinblick auf die Benachrichtigung reklamiert das Gutachten gesetzlichen Novellierungsbedarf. So müsse etwa sichergestellt werden,

dass die Verteidiger ihre Mandanten tatsächlich über die erfolgte Überwachung informieren. Auch müsse ein Kriterium bestimmt werden, ob und welche Dritte (also weder Tatverdächtige noch Anschlussinhaber), die abgehört worden waren, zu benachrichtigen seien. Gegebenenfalls sei zwischen privaten und geschäftlichen Kommunikationsinhalten zu unterscheiden (S. 471).[15] Im letzten Satz des Gutachtens wird aber auch hier der Praxis Vorrang eingeräumt: „Eine zwar in rechtsstaatlicher Weise normierte, aber tatsächlich nicht durchführbare Regelung erscheint als Provokation des Regelungsbruchs“ (S. 472).

Erfolge und der Sinn der TKÜ

Man könnte argumentieren, statt die Rechtswirklichkeit der TKÜ an demokratisch-rechtsstaatlichen Grundsätzen zu messen, sei es zeitgemäßer, sie nach ihren Erfolgen zu beurteilen. Die neuen Verbrechensformen verlangten eben nach einem neuen Rechtsstaatsverständnis, in dem die Bürgerrechte, Grundrechtsschutz, unabhängige Kontrollen, Gewaltenteilung etc. auf den Ehrenplatz in Sonntagsreden verwiesen werden müssen. Aber selbst auf der Ebene pragmatischer Effizienz ist die TKÜ bei Lichte betrachtet ein großer Misserfolg: Das Gutachten konnte den Ausgang der Verfahren gegen 1.065 überwachte Beschuldigte verfolgen. Die Verfahren gegen 534 Beschuldigte wurden von der Staatsanwaltschaft eingestellt; davon bei 433 mit der Begründung, dass kein genügender Anlass zur Klageerhebung gefunden werden konnte (S. 344f.). Im Klartext bedeutet das, dass rund 50 % der Abgehörten ohne jede strafrechtliche Relevanz belauscht wurden. Die Schlussfolgerung der GutachterInnen, die TKÜ finde „in der Praxis auch zielgerichtet und umsichtig Verwendung“ (S. 463), bleibt angesichts dieser Versagensquote ein Rätsel. Einem Postboten, der 50 % seiner Sendungen in falsche Briefkästen wirft, würde man wohl kaum attestieren, er handele „zielgerichtet und umsichtig“!

Um die tatsächlichen Effekte der TKÜ aufzuspüren, unterscheidet das MPI zwischen unmittelbaren, mittelbaren und sonstigen Erfolgen; außerdem wurden die Maßnahmen von der Polizei und den MPI-Auswertern bewertet. Während zu den unmittelbaren Erfolgen etwa

15 Bizer a.a.O. (Fn. 10) weist überzeugend nach, dass dieser Vorschlag der gefestigten Rechtsprechung des Bundesverfassungsgerichts zum Schutzbereich des Post- und Fernmeldegeheimnisses widerspricht.

„Entlastung“ oder „Selbstbelastung“ gezählt wurden, gehörten zu den mittelbaren Erfolgen die „Hinweise auf Straftaten Dritter“ oder Hinweise auf eine weitere Straftat. Die „sonstigen Erfolge“ stellten eine Restkategorie dar (S. 358f.). Nur in 302 der 501 ausgewerteten Verfahren (= 60,3 %) führte die TKÜ überhaupt zu irgendeiner Art von Erfolg (S. 368). Aufgeschlüsselt nach Erfolgsarten ergab die Analyse dieser 302 Verfahren, dass 62 % aller TKÜ-Erkenntnisse zu mittelbaren Erfolgen und nur 28 % zu unmittelbaren führten (S. 371), d.h. nur in 85 Verfahren wurden die Informationen gefunden, die man zu finden hoffte, während in 188 Verfahren „Zufallsfunde“ gemacht wurden. Die Bewertung durch die MPI-Auswerter bestätigt diese Zahlen: lediglich 26 % der TKÜs wurden als erfolgreich eingestuft. Diese Bilanz belegt sowohl die geringen Erfolge der TKÜ wie deren großes Ausforschungspotential.

Das Gutachten verfolgt den Weg der TKÜ-Erkenntnisse über das Strafverfahren bis zum Urteil und das Rechtsmittelverfahren: Die TKÜ wird nur bei 12 % der Beschuldigten als Beweismittel in der Anklage aufgeführt; in 38 % dieser Fälle maßen die MPI-Auswerter den TKÜ-Beweisen keinerlei Bedeutung für die Anlageschrift bei (S. 402). Nur bei 82 Beschuldigten wurden die TKÜ-Erkenntnisse im Urteil aufgegriffen. Gemessen an den 1.138 TKÜ-Beschuldigten des Jahres 1998 waren dies 7,2 Prozent. Die eigentliche Bedeutung der TKÜ liegt nach Ansicht der GutachterInnen darin, dass sie zur Erlangung anderer Beweise beiträgt. Dieser mittelbare Erfolg könne deshalb nicht an ihrer Erwähnung im Strafverfahren gemessen werden. Die enorme und effektlose „Streubreite“ der TKÜ, „die auch das soziale Umfeld der Zielperson einbezieht und sich damit insbesondere auf völlig unverdächtige Kommunikationsteilnehmer erstreckt“,[16] wird durch diese Einsicht aber nicht relativiert.

Mittelbare und unmittelbare Erfolge selbst werden keiner Würdigung unterzogen. Weder erfolgt ein Bezug auf die Schwere der Tat, noch auf die Wirkungen erfolgreicher Verurteilungen. Hinter dem neuen Nebelbegriff der „Transaktionskriminalität“ verschwinden die Maßstäbe für die Schwere der Taten. Zweifellos ist der Straßendeal eine Form der Transaktionskriminalität; aber sagt dies etwas über die Schwere der Tat, über die Verhältnismäßigkeit des Grundrechtseingriffs mittels TKÜ aus? Wenn die TKÜ vor allem zum strafverfolgerischen Eindringen in illegale Märkte eingesetzt wird, warum fragt das Gutachten dann an keiner Stelle danach,

16 Bizer a.a.O. (Fn. 10)

wie die Marktbedingungen durch die TKÜ verändert werden? Warum spielen die Erfolgsaussichten der Strafverfolgung in der Kontrolle illegaler Märkte keine Rolle für die „Effizienz-Bewertungen“ des MPI? Vermutlich scheute man diese Perspektive, weil die Bilanz der TKÜ dann noch verheerender ausgefallen wäre.

Ausführlich beschäftigt sich das Gutachten mit dem Begriff der Effizienz (S. 356 ff.). Einer Gegenüberstellung von Aufwand und gewünschtem Ertrag widersetzen sich die AutorInnen, weil der Polizei die Konkurrenz fehle und Marktmechanismen außer Kraft gesetzt seien (S. 357). Warum das Gutachten nicht wenigstens eine schlichte Aufwandsrechnung erstellt, bleibt unklar. Offenkundig hat man entsprechende Daten nicht erhoben. Auch die Angaben zu den Kosten der TKÜ sind mangelhaft. Lediglich auf die Dolmetscherkosten (zwischen 55 und 218.999 DM, S. 182) wird hingewiesen. Wenn man bedenkt, dass weniger als ein Drittel der TKÜs zu den erhofften Erfolgen führte, wäre eine finanzielle Kostenrechnung vermutlich nicht ganz uninteressant gewesen.

Reaktionen

Das MPI schließt sein Gutachten mit einer Reihe von Empfehlungen. Teilweise werden alternative Lösungen benannt, überall ist aber das Bemühen spürbar, der Praxis zu einer sicheren Rechtsgrundlage zu verhelfen. Am deutlichsten wird dies, wenn eine „Sonderbetrachtung“ für bestimmte Kriminalitätsformen ins Spiel gebracht wird (S. 465f.). Nachdem in den 80er Jahren die „vorbeugende Verbrechensbekämpfung“ den Polizeigesetzen zugeschlagen wurde, in den 90ern die StPO um verdeckte Methoden erweitert und der Informationsaustausch zwischen präventiv und repressiv gewonnenen Daten legalisiert wurde, soll nun ein präventiver Sonderbereich für die TKÜ im Strafprozessrecht geschaffen werden. Während die Praktiker übereinstimmend TKÜ-Regelungen für präventivpolizeiliche Zwecke ablehnen (S. 199f.) – denn sie empfinden etwa die Umgehung der Subsidiaritätsklausel als unproblematisch –, will das MPI ein rechtsstaatlich sauber geregeltes Überwachungs-Vorfeld. Wie die Untersuchung, so zeichnen sich die Vorschläge durch ihre „verfassungsrechtliche Maßstabslosigkeit“ (Bizer) aus.

Die Justizministerin hat angekündigt, die Mängel in der richterlichen Anordnung und in der Benachrichtigungspflicht auf Novellierungsbedarf

zu prüfen. Die Datenschutzbeauftragten,[17] die Bundestagsfraktionen von Bündnis 90/Die Grünen[18] und die der FDP[19] haben weitergehende Reformen gefordert. Ihre Wünsche beziehen sich durchweg auf die Anforderungen an die Begründung von TKÜ-Anträgen, auf die Qualität der richterlichen Entscheidung (Kollektivorgan, besonders qualifizierte Richter), auf die Einführung von Berichtspflichten, auf die Dauer der Überwachungsmaßnahmen, auf Verwertungs- und Beweismittelverbote oder auf die Reduzierung des Straftatenkatalogs.

Die Vorschläge gehen regelmäßig über das vom MPI angebotene Repertoire hinaus. Aber sie bleiben in dessen Horizont. Wie im MPI-Gutachten, so spielen die abhörenden Polizeien auch in der Reformdiskussion keine Rolle. Sofern man überhaupt etwas ändern wird, ist absehbar, dass der bürokratische Aufwand der TKÜ-Antragstellung erhöht wird, ohne dass der Unkultur der Überwachung entgegenwirkt wäre. Hier wäre der Platz für internationale Vergleiche gewesen. So bedeutet etwa das US-amerikanische Minimierungsgebot, dass die abgehörten Gespräche mitgehört werden müssen, die Überwachung sofort abgeschaltet werden muss, wenn das Gespräch irrelevant ist und nur das aufgezeichnet wird, was für das Verfahren von Bedeutung ist. Allein eine solche Vorschrift würde die Zahl der Überwachungen reduzieren, es würde die Praktiker vor Ort zu einer Abwägung von Aufwand, Anlass der Überwachung und Erfolgsaussicht veranlassen, bevor sie einen Antrag stellen. Und schließlich würde es die Streubreite mittelbarer TKÜ-Erkenntnisse verringern und die Benachrichtigungsproblematik erheblich verkleinern. Aber so zu verfahren, hieße ja, tatsächlich aus Erfahrungen lernen zu wollen, statt bestehende Praktiken zu legitimieren.

Norbert Pütter lehrt Politikwissenschaft an der Fachhochschule für Verwaltung und Rechtspflege Berlin und ist Redakteur von Bürgerrechte & Polizei/CILIP.

17 Entschließung der Datenschutzbeauftragten des Bundes und der Länder v. 25./26.9. 2003, www.baden-wuerttemberg.datenschutz.de/ds-konferenz/okt2003/mpi-tk.html

18 Positionspapier zur Telefonüberwachung v. 7.5.2003, in: Telefonüberwachung reformieren, Pressemitteilung 300/2003 v. 15.5.2003 (Anlage)

19 BT-Drs. 15/1583 v. 24.9.2003

Inland aktuell

Anti-Castor-Proteste 2003

Mit dem Transport von hochradioaktivem Müll ins Zwischenlager Gorleben Anfang November war im Wendland der alljährliche Ausnahmezustand angesagt. Begründet mit den üblichen Verdächtigungen, bildete wie jedes Jahr die Allgemeinverfügung eines Versammlungsverbots entlang der Transportstrecke und in einem weiten Umfeld um die atomtechnischen Anlagen den polizeilichen Auftakt. Zum ersten Mal seit Beginn der Castor-Transporte stellte der Einsatzleiter allerdings im Verlauf des Transportes und der trotz des Verbots stattfindenden Proteste fest, dass dieser Protest friedlich, sympathisch und fair sei.

Theoretisch war damit die Allgemeinverfügung hinfällig. Dass sie nicht aufgehoben wurde, lag vor allem daran, dass sie der Polizei die Möglichkeiten gab, nach eigenem Gutdünken zu handeln. Sie konnte Proteste zulassen oder Verbote mit Gewalt durchsetzen und die DemonstrantInnen in Gewahrsam nehmen. Während so die rechtliche Bandbreite polizeilichen Handelns entgrenzt wurde, mussten sich die BürgerInnen in einem unsicheren rechtsfreien Raum bewegen.

Noch während der Einsatzleiter die friedliche Qualität der Proteste lobte, wurde eine angemeldete Demonstration zur Ankunft der Castoren in Dannenberg wegen des angeblich drohenden „polizeilichen Notstands“ verboten. Trotzdem waren Proteste in der Nähe des Verladekrans und auf der Straßentransportstrecke möglich.

Die Rechtlosigkeit der BürgerInnen wurde dagegen richtig deutlich, als der Transport die letzten Kilometer auf der Straßentransportstrecke zurücklegen sollte. Bayerische Unterstützungskommandos drohten den TeilnehmerInnen einer Sitzblockade in Grippel mit härtester körperlicher Gewalt, sollten sie die Straße nicht freiwillig verlassen. Alle BürgerInnen dieses Dorfes wurden ohne Ankündigung und ohne Möglichkeit, den Ort zu verlassen, in Kessel verbracht. Hierfür wurden Privatgrundstücke genutzt und Zäune zerstört. EinwohnerInnen durften entweder nicht in ihre Häuser oder diese nicht verlassen. In Laase – außerhalb der Demonstrationsverbotszone – war eine Kulturveranstaltung geplant. Hier kes-

selte die Polizei das ganze Dorf ein. Sie ließ die Leute zwar in diesen Kessel hinein, aber über Stunden nicht mehr heraus. Insgesamt boten die Polizeieinsätze im Wendland ein Bild der Willkür.[1]
(Elke Steven)

Schleierfahndung im BGS-Gesetz verlängert

Die Befugnis des Bundesgrenzschutzes (BGS) zu sog. lageabhängigen Kontrollen in Zügen und Bahnanlagen sowie auf internationalen Flughäfen (§ 22 Abs. 1a BGS-Gesetz) war bei ihrer Einführung 1998 bis zum 31.12.2003 befristet worden. Vor Ablauf sollte die Bundesregierung eine Evaluation über die Anwendung vorlegen, was Anfang September mit einem 15-seitigen Bericht des Bundesinnenministeriums (BMI) geschehen ist. Dass es sich dabei nicht um eine unabhängige Evaluierung nach überprüfbaren Kriterien handelt, lässt schon der Titel „Erfahrungsbericht“ vermuten. Neben einer 7-seitigen „Statistischen Übersicht“ zur Anzahl der Personenkontrollen und den dabei festgestellten Straftaten, Ordnungswidrigkeiten und Personenfahndungserfolgen liefern die übrigen acht Seiten wahllos herausgegriffene „Erfolge“ sowie wenige Absätze zum Beschwerdeverhalten, zu Fortbildungsmaßnahmen der Polizei, zur Zusammenarbeit mit anderen Behörden und zur Öffentlichkeitsarbeit. In der abschließenden knappen Bewertung kommt der Bericht denn auch zu dem Ergebnis, dass die Befugnis vom gesamten BGS positiv bewertet und als „wertvolles Instrument zur Bekämpfung der unerlaubten Einreise sowie der Schleusungskriminalität anerkannt“ wird. Schließlich stießen die Kontrollen auch bei der Bevölkerung auf positive Resonanz und trügen „wesentlich zur Erhöhung des Sicherheitsgefühls“ bei.

Offenbar evaluiert sich hier der BGS selbst. Anderenfalls relativierten sich die Ergebnisse erheblich. Nach BGS-Gesetz darf der BGS allein zur „Verhinderung oder Unterbindung der unerlaubten Einreise“ nach Deutschland lageabhängig kontrollieren. Bei den zwischen 1999 und 2002 durchgeführten 1.185.460 Kontrollen wurden jedoch lediglich 6.789 „unerlaubte Einreisen“ festgestellt. Das entspricht einer Quote von 0,57 %. Sie sank von 1,15 % im Jahr 1999 auf 0,25 % im Jahr 2002. Hingegen ergab sich bei Kontrollen in knapp 5 % der Fälle allgemein ein Verdacht auf eine Straftat, in 3,8 % auf eine Ordnungswidrigkeit. Damit

1 weitere Informationen beim Komitee für Grundrechte, info@grundrechtekomitee.de

werden sog. Zufallsfunde zum eigentlichen Ziel der Überprüfungen. Nicht umsonst bezeichnet der BGS im Bericht die Kontrollen „als sehr geeignete Einstiegsbefugnis“. Der Rand der Legalität ist damit überschritten.

Während sich BGS und BMI ihre „Treffer“-Zahlen schön interpretieren, kommen sie beim Beschwerdeaufkommen ganz ohne aus. Es wird schlicht vom BGS selbst als „gering“ bezeichnet. Dass darüber gar keine Statistik geführt wird, gab die Bundesregierung als Antwort auf eine Kleine Anfrage (BT-Drs. 14/3990) zu. Auch die Vorwürfe wegen der zumeist selektiven, rassistischen Kontrollpraxis weist der Erfahrungsbericht lapidar zurück, indem er Initiativen wie KOGAMRA oder „Bürger beobachten den BGS“ pauschal als BGS-feindlich diskreditiert. Im selben Bericht ist jedoch von „Profilpersonen“ die Rede, bei denen eine Vielzahl „qualifizierter Treffer“ erzielt werden konnte. Dass damit ein Selektionsraster im Sinne äußerer Merkmale wie Hautfarbe, Kleidung, Auftreten etc. gemeint ist, hat die Polizei an anderer Stelle mehrfach zugegeben.[2] Aber auch über die Staatsangehörigkeit der Kontrollierten wird keine Statistik geführt.

„Rechtssicher und sensibel“ würden die BGS-Kontrollen laut der Selbstevaluation durchgeführt. Es war sicher nur ein Versehen, dass ein BGS-Beamter bei einer von einem CILIP-Redaktionsmitglied miterlebten Kontrolle behauptete, es gebe eine Pflicht, einen Ausweis bei sich zu tragen.

Dass zumindest DIE GRÜNEN dieser Evaluation nicht ganz trauen, zeigt der im November verabschiedete Gesetzentwurf der Bundesregierung, der eine weitere Befristung der Befugnis bis zum 30.6.2007 vorsieht. Darin ist eine erneute Evaluation ausdrücklich festgeschrieben. Sie soll statistisch aufschlüsseln, wie viele Ermittlungen eingeleitet wurden, für die der BGS zuständig ist, und wie viele Zufallstreffer es gab. Erhoben werden soll auch, inwiefern die Kontrollen auf konkreten Lagebildern beruhen, die Anzahl der Beschwerden und die negativen Auswirkungen auf Reisende, z.B. durch Reiseunterbrechungen, weil der/die Kontrollierte keine Ausweisdokumente bei sich hatte. Von einer unabhängigen Bewertung ist aber auch hier keine Rede. Selbst die ist nicht immer ein Garant für eine unparteiische Evaluation, wie das Gutachten des Max-Planck-Instituts zur Telefonüberwachung zeigt (siehe S. 73-84 in diesem

2 vgl. Kant, M.: Verdachtsunabhängige Kontrollen, in: Bürgerrechte & Polizei/CILIP 65 (1/2000), S. 29-35 (30)

Heft). Eine ernst gemeinte Evaluation der Schleierfahndung müsste in jedem Fall die Folgen für MigrantInnen berücksichtigen.
(Martina Kant)

Lauschangriffe 2002

Ende August 2003 erstattete die Bundesregierung ihren Bericht über die akustische Wohnraumüberwachung.[3] Danach griffen die Strafverfolgungsbehörden im Jahr 2002 in insgesamt 30 Verfahren zum Mittel des großen Lauschangriffs nach § 100c Abs. 1 Nr. 3 StPO. Die Maßnahmen richteten sich gegen 33 Wohnungen, die zwischen null und 82 Tagen überwacht wurden (durchschnittliche Dauer 24 Tage). Betroffen waren 97 Personen (davon 14 Nichtbeschuldigte). In zehn Verfahren waren die Betroffenen zum Zeitpunkt des Berichts wegen andauernder Ermittlungen noch nicht benachrichtigt. Bayern führt die Statistik mit sieben Fällen und 18 Betroffenen an. Zehn weitere Länder setzten den großen Lauschangriff in jeweils zwischen einem und drei Verfahren ein. Hinzu kommen zwei Verfahren, die der Generalbundesanwalt führte. Lauschangriffe zur Gefahrenabwehr betrieben die Bundespolizeien nicht.

Die wichtigsten Anlassstraftaten waren wie im Jahr zuvor Mord/ Totschlag/Völkermord und Betäubungsmitteldelikte (jeweils neun Nennungen). In sieben Fällen gingen die StrafverfolgerInnen von kriminellen oder terroristischen Vereinigungen aus. In 17 Verfahren sahen sie eine „OK-Relevanz“ gegeben. In zwölf der 30 Fälle führte die Überwachung nicht zu verfahrensrelevanten Ergebnissen. In zehn Verfahren waren dafür „inhaltliche Gründe“ ausschlaggebend. Die Kosten berechnen die Justizverwaltungen offenbar nach wie vor anhand unterschiedlicher Kriterien: Hamburg berechnete für eine 71-tägige Überwachung 1.000 Euro, Bayern für eine zweitägige dagegen 6.650 Euro. Die Kosten pendeln zwischen 1 und 300 Euro pro Maßnahmetag, die Angaben sind deshalb ohne eine genauere Aufschlüsselung wertlos. Insgesamt vermittelt der Bericht allenfalls einen vagen Eindruck von der Praxis der Behörden. Für eine ernsthafte parlamentarische Kontrolle ist er unbrauchbar.
(Stephan Stolle)

Erlass in Niedersachsen zwingt Schulen zur Anzeige

3 BT-Drs. 15/1504 v. 28.8.2003

Das Niedersächsische Kultusministerium hat in Zusammenarbeit mit dem Innen- und dem Justizministerium einen Runderlass herausgegeben, demzufolge die Schulleitungen verpflichtet sind, die Polizei zu informieren, sobald sie Kenntnis von einer Straftat an ihrer Schule erhalten.[4] Polizei und Staatsanwaltschaft sind ihrerseits verpflichtet, den Schulen Daten delinquenter SchülerInnen zu vermitteln. Gemeldet werden sollen u.a. Straftaten gegen das Leben, Raubdelikte, gefährliche Körperverletzungen oder andere Gewaltdelikte sowie Bedrohung, Beleidigung (z.B. Sexualbeleidigung), Sachbeschädigung (z.B. Graffiti), Nötigung oder der Umgang mit Betäubungsmitteln. Auch Bagatelldelikte, die sonst die Schule selbst regelte, werden so zu Straftaten.

Die MinisterInnen begründen ihren Erlass mit einer Messerstecherei in einer hannoveranischen Realschule Ende August, bei der ein 15-Jähriger durch einen Mitschüler lebensgefährlich verletzt wurde. „Schule, Polizei und Staatsanwaltschaft haben ... das gemeinsame Ziel, die Sicherheit der Schülerinnen und Schüler beim Schulbesuch zu gewährleisten und Straftaten im Lebensraum Schule ... und ... außerhalb der Schule zu verhüten“, so heißt es im Erlass.

Die Gewerkschaft Erziehung und Wissenschaft (GEW) lehnte in einer Erklärung vom 3.12.2003 den Erlass ab und kritisiert die „Demonstration von staatlicher Gewalt“ anstelle des Primats von Prävention.[5] In der Tat: Wie sollen SchülerInnen Vertrauen erlangen, wenn ihre LehrerInnen sie jederzeit öffentlich denunzieren müssen und somit zu Handlangern von Polizei und Justiz werden? Die Kriminalisierung von SchülerInnen wird zu einer Zunahme der statistischen Delinquenz, nicht aber zu einer Abnahme begangener Straftaten führen. Das niedersächsische Kultusministerium, so beklagte die GEW bereits am 19.8.2003, hat die Stellen für SozialpädagogInnen an Hauptschulen gestrichen und die Gelder für LehrerInnenfortbildungen gekürzt.
(Marion Knorr)

4 Gem. RdErl. des MK (201-51 661), des MI (23-51603/4-1) und des MJ (4210 – S 3.202) v. 30.9.2003

5 www.gew-nds.de/Aktuell/aktuell.html

Meldungen aus Europa

Datenbestände im SIS

Auf eine Anfrage der PDS-Abgeordneten Petra Pau hat das Bundesinnenministerium den Bestand der zum Jahresbeginn 2003 im Schengener Informationssystem (SIS) gespeicherten Ausschreibungen mitgeteilt.[1] Von den 9,7 Mio. Sachfahndungsdaten bezogen sich allein 7,6 Mio. auf Identitätspapiere, was sich daraus erklärt, dass alle verloren oder gestohlen gemeldeten Personalausweise und Pässe im SIS erfasst werden.

Sach-fahndung	Fahrzeuge	Schuss-waffen	Blanko-dokumente	Identitäts-papiere	Bankno-ten	Gesamt
SIS gesamt	1.106.626	301.348	265.929	7.687.008	380.710	9.741.511
Dt. Daten	150.217	143.966	141.514	1.514.427	208.500	2.158.624

Die rund 1,2 Mio. Personendaten bezogen sich auf 874.032 reale Personen. Von denen waren gerade einmal 1,6 Prozent zur Festnahme und Auslieferung (Art. 95), dagegen 89 Prozent zur Einreiseverweigerung (Art. 96 Schengener Übereinkommen) ausgeschrieben.

Personenfahndung	SIS gesamt	Deutsche Daten
Festnahme/Auslieferung (Art. 95)	13.826	4.155
Einreiseverweigerung (Art. 96)	775.868	269.359
Vorläufige Ingewahrsamnahme, Jugendliche (Art. 97)	16.983	1.079
Vorläufige Ingewahrsamnahme, Erwachsene (Art. 97)	16.598	1.167
Aufenthaltsermittlung (Art. 98)	34.379	2.752
Polizeiliche Beobachtung (Art. 99 II)	10.821	544
Beobachtung, Geheimdienste (Art. 99 III)	5	0
Gezielte Kontrolle (Art. 99 II)	5.552	0
Personen gesamt	**874.032**	**279.056**
Alias-Identitäten	392.650	328.166
Personendatensätze total	**1.266.682**	**607.222**

Nach wie vor ist damit das SIS nur am Rande ein System zur Fahndung nach StraftäterInnen, in erster Linie aber ein technisches Instrument der rigiden Migrations- und Asylpolitik. Die Ausschreibung abgewiesener

1 BT-PlProt. 15/62 v. 24.9.2003, S. 5264f.

Asylsuchender erklärt auch den hohen Anteil der Alias-Identitäten. Am SIS sind zwar insgesamt 15 Staaten beteiligt. Bezeichnenderweise sind jedoch 35 Prozent der Art. 96-Daten und 80 Prozent der Alias-Identitäten von Deutschland eingegeben worden.

Aufbauplanung für das SIS II

Ende 2006 soll das Schengener Informationssystem der zweiten Generation einsatzbereit sein. So ist es zumindest in den Schlussfolgerungen über die „Funktionen" und die „Architektur" des neuen Systems vorgesehen, die der Rat auf seiner Juni-Sitzung verabschiedet hat.[2] Demnach soll das SIS weiterhin ein „hit/no hit"-System, also ein bloßes Abfragesystem bleiben, allerdings für neue „Funktionen" offen sein: Der Rat will „rechtzeitig zur ersten Freigabe des SIS II erforderlichenfalls durch Rechtsakte" darüber befinden, welche neuen Datenkategorien (z.B. über „gewalttätige Randalierer") und Datenfelder (für digitalisierte Fotos und andere biometrische Daten) zu schaffen sind und welche zusätzlichen Behörden vollen oder teilweisen Zugriff zum SIS erhalten sollen.

Einen ersten „Rechtsakt" hat der Rat bereits gebilligt. Er änderte per „Beschluss" auf spanische Initiative das Schengener Durchführungsübereinkommen: Demnach sollen neue Datenkategorien in der Sachfahndung (für Container, Luft- und Wasserfahrzeuge, Schecks, Kreditkarten und Wertpapiere) entstehen. Zugriff zu den Daten erhalten auch die Staatsanwaltschaften sowie Europol und Eurojust. Für den Anschluss der letzteren bedarf es allerdings zusätzlich einer Änderung der Europol-Konvention bzw. des Beschlusses über Eurojust. Diese Änderungen könnten schon im Rahmen des bestehenden SIS eingeführt werden, weitere „Funktionen" für das SIS II sollen die zuständigen Ratsarbeitsgruppen möglichst rasch ausarbeiten.[3]

Für das SIS II ist nicht nur eine zentrale Einheit (C.SIS) geplant, sondern zusätzlich ein „Notfallsystem". Gegebenenfalls könnten „im operativen Betrieb die Abfragen auf beide Systeme verteilt werden." Das C.SIS verbleibt voraussichtlich in Strasbourg, für die zweite Zentrale hat Österreich einen Standort angeboten: ein „Ausweichrechenzentrum ... das sich in einer verbunkerten, baulich besonders gesicherten, unterirdischen

2 EU-Ratsdok. 9845/03 v. 5./6.6.2003
3 EU-Ratsdok. 10054/03 v. 24.6.2003

Anlage der militärischen Luftraumüberwachung in einem Berg in den Alpen“ befindet und „verlässlichen“ Schutz gegen „Angriffe von außen“ bietet. Alarmpläne „im Falle von terroristischen Bedrohungen, zivilen Übergriffen oder Demonstrationen“ seien vorhanden. Das SIS II und das in Planung befindliche neue Visuminformationssystem (VIS) sollen auf der gleichen „technischen Plattform“ betrieben werden. Das militärische Loch in den Salzburger Alpen habe, so die österreichische Delegation, auch Platz für das Back up-System des VIS.[4]

Europäische Katastrophen: Demos und Fußballspiele

In einer kurz vor der Verabschiedung stehenden Entschließung „über die Sicherheit von Tagungen des Europäischen Rates und anderer Veranstaltungen“ bekräftigt der Rat die mittlerweile sattsam bekannten Rezepte im Umgang mit grenzüberschreitenden Demonstrationen. Dazu gehört an vorderster Stelle die Ausnahmeklausel in Art. 2 Abs. 2 des Schengener Durchführungsübereinkommens, nach der die Mitgliedstaaten für begrenzte Zeit auch ihre Binnengrenzen wieder kontrollieren dürfen. Statt generalisierter Kontrollen und dem damit verbundenen Verkehrschaos empfiehlt er eine Selektion: Durch „erkenntnisgestützte Kontrollen“ soll die Polizei bereits an den Grenzen Personen herausfiltern, gegen die „der begründete Verdacht“ besteht, dass sie „die öffentliche Ordnung und die Sicherheit der Veranstaltung stören“ wollen. Der „gastgebende Staat“ soll dazu von seinen EU-Partnern Namen und sonstige Informationen über die vermuteten Unruhestifter erhalten und kann sich von polizeilichen Verbindungsbeamten der Nachbarstaaten assistieren lassen.[5]

Ende November 2002 hatten die Minister bereits einen „Leitfaden für die Sicherheit“ von Gipfeltreffen gut geheißen, der in weiten Teilen die Regelungen einer Gemeinsamen Maßnahme von 1997 wiederholte: Aufbau von nationalen Kontaktstellen, Austausch von Daten und Einschätzungen („Risikoanalysen“) im Vorfeld von Demonstrationen, Grenzkontrollen, Entsendung von Verbindungsbeamten. Neu war an dem Leitfaden nur, dass auch Europol Analysen über zu erwartende Gefahren

4 EU-Ratsdok. 12367/03 v. 9.9.2003
5 EU-Ratsdok. 13195/03 v. 4.11.2003

liefern sollte, obwohl das Amt gemäß Konvention nur für Fälle der organisierten Kriminalität und des Terrorismus zuständig ist.[6]

Auf einem ähnlichen Modell beruht seit Jahren die polizeiliche Zusammenarbeit anlässlich größerer Sportereignisse. Als nationale Kontaktstelle fungiert dabei in Deutschland die „Zentrale Informationsstelle Sporteinsätze" beim nordrhein-westfälischen Landeskriminalamt, die anfänglich auch die mittlerweile beim Bundeskriminalamt geführte Datei „Gewalttäter Sport" betreute. Die auf privatrechtlicher Basis vom Deutschen Fußballbund ausgesprochenen Stadionverbote führten fast automatisch zu einer Speicherung in der Datei.

Die Polizei-Arbeitsgruppe des Rates empfiehlt nun, insbesondere im Hinblick auf die Europameisterschaft 2004 in Portugal und die Weltmeisterschaft 2006 in Deutschland, dieses System der Stadionverbote per Ratsbeschluss in der ganzen EU zu übernehmen. Stadionverbote sollen vorrangig gegen Personen verhängt werden, die sich eines gewaltsamen Verhaltens bei Fußballspielen „schuldig" gemacht haben. Ob damit eine rechtskräftige Verurteilung oder – entsprechend der deutschen und der britischen Praxis – ein seitens der Polizei und/oder der Sportverbände ausgesprochener Verdacht genügt, ist dem englischen Text nicht eindeutig zu entnehmen. Nationale Stadionverbote, so will die Mehrheit der Arbeitsgruppe, sollen auch international durchgesetzt werden und bei Zuwiderhandlungen Geldbußen nach sich ziehen. Die nationalen Fußballkontaktstellen sollen den dafür erforderlichen Datenaustausch organisieren. Die Daten – so die Beschwichtigung – dürften nur für die Verweigerung des Einlasses oder für andere „angemessene" Maßnahmen zur Aufrechterhaltung von Recht und Ordnung verwendet werden. Soweit erkennbar hat bisher nur Schweden diesen Plänen widersprochen.[7]
(sämtlich: Heiner Busch)

6 EU-Ratsdok. 12637/2/02 v. 12.11.2002
7 EU-Ratsdok. 10966/1/03 v. 22.7.2003, 11843/03 v. 29.7.2003, 12182/03 v. 3.9.2003

Chronologie

zusammengestellt von Marion Knorr

Juli 2003

01.07.: **Lichtenhagen-Prozess beendet:** Der Bundesgerichtshof (BGH) beendet das letzte Verfahren wegen der rassistischen Krawalle in Rostock-Lichtenhagen von 1992. Er verwirft die Revision gegen ein Urteil des Landgerichts (LG) Schwerin, das im Juni 2002 drei zur Tatzeit 17-19-jährige Männer wegen versuchten Mordes und schwerer Brandstiftung zu ein bis anderthalb Jahren Jugendstrafe auf Bewährung verurteilt hatte.

03.07.: **Verschärftes Sexualstrafrecht:** Der Bundestag führt neue Straftatbestände für sexuellen Missbrauch von Kindern ein und erhöht die Mindeststrafe für schweren sexuellen Missbrauch von einem auf zwei Jahre Gefängnis. Eine Anzeigepflicht für Personen, denen ein Missbrauchsfall bekannt wird, wird nicht eingeführt.

09.07.: **Haft für Stralsunder Polizisten**: Das LG Stralsund verurteilt zwei Polizisten, die Ende 2002 einen betrunkenen Obdachlosen am Stadtrand ausgesetzt hatten, zu drei Jahren Haft. Der 35-Jährige war erfroren.

10.07.: **Sachsens Polizeigesetz teilweise verfassungswidrig:** Der Sächsische Verfassungsgerichtshof erklärt eine Regelung für nichtig, wonach BürgerInnen nicht nachträglich informiert werden müssen, wenn der Einsatz verdeckter Ermittler gefährdet wäre. Schleierfahndung und Videoüberwachung seien dagegen verfassungskonform.

14.07.: **Bewährung für Erfurter Polizisten:** Ein Hamburger Amtsgericht verurteilt drei Thüringer Polizisten wegen Körperverletzung im Amt zu je einem Jahr Haft auf Bewährung. Im November 2002 hatten sie bei einer Demonstration in Hamburg zwei Zivilpolizisten verprügelt.

15.07.: **Schmerzensgeld für Prügel:** Aufgrund eines zivilgerichtlichen Vergleichs muss die Stadt Bremen einem Studenten, der an Sylvester 1999 auf einer Polizeiwache verprügelt worden war, 4.250 Euro Schmer-

zensgeld zahlen. Das Strafverfahren gegen die beschuldigten Beamten war hingegen eingestellt worden.

16.07.: **Verfassungsbeschwerde gegen Handy-Ortung**: Die Humanistische Union (HU) reicht Verfassungsbeschwerde gegen den Einsatz des IMSI-Catchers ein. Der Einsatz des Gerätes, das alle Handys in der Nähe orten und abhören kann, verstoße gegen das Fernmeldegeheimnis.

17.07.: **Deutsch-polnisches Rechtshilfeabkommen unterzeichnet:** Der Vertrag regelt u.a. die grenzüberschreitende Telefonüberwachung.

22.07.: **Klage gegen Videokontrolle abgewehrt:** Nach einer Entscheidung des Verwaltungsgerichtshofes Baden-Württemberg können Städte und Gemeinden Kriminalitätsbrennpunkte weiter per Videokamera überwachen. Ein „überwiegendes Allgemeininteresse“ mache Einschränkungen für Einzelne nötig.
Auslieferung trotz Foltergefahr: Das Bundesverfassungsgericht (BVerfG) verwirft die Beschwerde eines des Betruges Beschuldigten gegen seine Auslieferung nach Indien. Der deutsch-indische Auslieferungsvertrag von 2001 sei ein Indiz für die Achtung der Menschenrechte in dem Land. Die Klage hatte auf Berichte von Amnesty International und des Auswärtigen Amtes verwiesen, wonach Folter eine von der indischen Polizei „häufig angewandte Vernehmungsmethode“ sei.

24.07.: **„Überreaktion im Stress“:** Ein Berliner Kriminalpolizist, der im Oktober 2002 einem bereits Festgenommenen durch einen Tritt ins Gesicht den Kiefer gebrochen hatte, wird zu elf Monaten Gefängnis auf Bewährung verurteilt; er entgeht damit einer Entlassung.

25.07.: **Bewährungsstrafen für Kölner Polizisten:** Das LG Köln verurteilt sechs Polizisten wegen gemeinschaftlicher Körperverletzung im Amt mit Todesfolge zu Strafen zwischen sechs und zwölf Monaten auf Bewährung. Sie hatten 2002 den 31-jährigen Stephan N. im Polizeiauto und auf der Kölner Eigelsteinwache so schwer misshandelt, dass er nach zweiwöchigem Koma starb (vgl. CILIP 72, S. 84).

28.07.: **Urteil zu WM-Krawallen in Frankreich:** Das LG Bochum verurteilt einen 28-Jährigen zu 40 Monaten Haft. Bei den Krawallen an der Fußball-WM 1998 habe er zwar nicht selbst den Polizisten Daniel Nivel angegriffen, aber das brutale Vorgehen von vier anderen bereits verurteilten Hooligans gebilligt. Die Verteidigung kündigt Revision an.

29.07.: **Urteil im Metzler-Prozess:** Das LG Frankfurt verurteilt den 28-jährigen Magnus Gäfgen wegen Entführung und Ermordung des elfjährigen Jakob von Metzler zu lebenslanger Haft. Die Verteidigung hatte zu Beginn des Verfahrens eine Einstellung gefordert, weil dem Beschuldigten während der Vernehmung im Oktober 2002 auf Anordnung des Frankfurter Polizeivizepräsidenten mit Folter gedroht worden war.

30.07.: **Beschlagnahmeprivileg von Abgeordneten:** Auch die Büros der Mitarbeiter von Abgeordneten sind vor Beschlagnahme geschützt. Das BVerfG gibt der Verfassungsbeschwerde des SPD-Obmanns im Parteispendenausschuss Frank Hofmann statt. Er hatte gegen die Durchsuchung von Bundestagsbüro und Wohnung eines Mitarbeiters der SPD-Arbeitsgruppe im Ausschuss geklagt. (Az.: 2 BvR 508/01-2 BvE 1/01)

August 2003

04.08.: **Mehrjährige Haft für Neonazi:** Das LG Berlin verurteilt einen Neonazi wegen mehrfacher gefährlicher Körperverletzung, Volksverhetzung und Beleidigung zu sechs Jahren und drei Monaten Haft. Der 23-Jährige war seit 2001 an zahlreichen Gewalttaten beteiligt.

06.08.: **Gefängnis für Ersttäter:** Sachsen führt in einem Modellprojekt ein eigenes Gefängnis für „Ersttäter“ ein, das „kriminelle Ansteckung“ vermeiden soll und für 300 Gefangene Platz bietet.

09.08.: **Grenzcamp aufgelöst**: Erst nach 17 Stunden beendet die Polizei die Einkesselung eines Grenzcamps gegen die restriktive Flüchtlingspolitik in Köln. Den TeilnehmerInnen war zuvor das Wasser abgestellt worden. Nur wer sich fotografieren ließ und seine Personalien angab, durfte den Kessel verlassen.

14.08.: **Klage von NPD-Spitzel:** Der NPD-Funktionär und ehemalige Verfassungsschutz-Spitzel Wolfgang Frenz verklagt das Land Nordrhein-Westfalen auf Schadensersatz. Durch das Auffliegen seiner V-Mann-Tätigkeit habe seine Heilpraxis viele Patienten verloren; das Landesamt für Verfassungsschutz habe seine Geheimhaltungsvorschriften verletzt. Am 3.12. lehnt das LG Düsseldorf Forderungen des Ex-V-Mannes ab.
Berlin stoppt Überwachung von Scientology: Der Berliner Verfassungsschutz beendet die Beobachtung der Sekte und greift damit einem Urteil des Verwaltungsgerichts (VG) vor. Dieses hatte schon 2001 den weiteren Einsatz von V-Leuten gegen die Sekte untersagt.

15.08.: **Häuserräumung rechtswidrig:** Es wird bekannt, dass das VG Berlin im Juli 2003 einem ehemaligen Bewohner der Rigaer Straße 80 rechtgegeben und die Räumung des besetzten Hauses im Jahre 1997 für rechtswidrig erklärt hat. (Az.: VG 1 A 321.98)

19.08.: **Schill entlassen:** Hamburgs Erster Bürgermeister entlässt Innensenator Roland Schill. Dessen Nachfolger wird am 3.9. der ebenfalls der Schill-Partei angehörende Dirk Nockemann.

23.08.: **Iris-Erkennung auf dem Flughafen Frankfurt:** Das Bundesinnenministerium (BMI) kündigt einen im September startenden sechsmonatigen Feldversuch an, bei dem VielfliegerInnen nur einer automatisierten Grenzkontrolle per Iris-Erkennung unterworfen werden. Die biometrischen Daten werden auf einer Chipkarte gespeichert.

27.08.: **Metin Kaplan darf bleiben:** Laut Urteil des VG Köln habe der Islamist Metin Kaplan zwar keinen Asylanspruch, dürfe aber wegen der ihm in der Türkei drohenden Folter nicht abgeschoben werden. Am 18.10. bestätigt das BVerfG das Verbot von Kaplans „Kalifatstaat".
Verdacht der Misshandlung: Braunschweiger Polizisten misshandelten nach Angaben des niedersächsischen Flüchtlingsrats einen nigerianischen Mann, der nach einer Verkehrskontrolle auf die Wache verbracht wurde, wo er sich ausziehen musste und von fünf Beamten getreten und geschlagen wurde. Die Staatsanwaltschaft bestätigt später Wunden und Prellungen am ganzen Körper des Mannes. Sie ermittelt sowohl gegen die Beamten als auch wegen Widerstandes gegen den Nigerianer.

September 2003

04.09.: **Keine Abschiebungen in den Kongo:** Vorerst schiebt Berlin keine Menschen mehr in die Demokratische Republik Kongo ab. Ein noch am 30.8. abgeschobener 37-jähriger Kongolese war bei seiner Ankunft in Kinshasa festgenommen und misshandelt worden. Innensenator Körting (SPD) lässt die Lage nun durch das Auswärtige Amt prüfen.
Haft für irakische Botschaftsbesetzter: Das LG Berlin verhängt gegen fünf Exil-Iraker Strafen von jeweils drei Jahren Haft. Sie hatten ein Jahr zuvor die irakische Botschaft in Berlin demonstrativ besetzt.
Erfolg für Castor-GegnerInnen: Das LG Lüneburg, so wird jetzt bekannt, hat im August Urteile des Amtsgerichts (AG) Dannenberg aufgehoben. Atomkraft-GegnerInnen hatten gegen Massenfestnahmen bei

den Anti-Castor-Protesten 2001 und 2002 geklagt, waren aber vom AG nicht persönlich angehört worden.

Aktenfälschen zum Abschieben: Pro Asyl rügt ein Urteil des AG Cloppenburg. Das Gericht hatte einen Beamten der Kreisverwaltung Cloppenburg (Niedersachsen) freigesprochen, der im Jahr 2000 einem abgelehnten Asylbewerber frei erfundene Personendaten zugeschrieben hatte, damit er abgeschoben werden konnte. (Az.: 3 Ls 131 Js 35096/00)

08.09.: **Keine Anklage gegen Seidler:** Das Verfahren gegen Christoph Seidler wegen gemeinschaftlichen Mordes an dem Bankier Alfred Herrhausen 1989 wird von der Bundesanwaltschaft eingestellt. Der Haftbefehl gegen den heute 45-Jährigen war bereits aufgehoben worden, als er sich 1996 den Behörden stellte.

09.09.: **Asylstatistik veröffentlicht:** Laut Statistik des BMI ist die Zahl der Asylsuchenden in Deutschland auf den niedrigsten Stand seit 1987 gesunken. Die Anerkennungsquote liegt bei nur 1,7 %.

12.09.: **Videoüberwachung auf Bahnhöfen verschärft:** Es wird bekannt, dass ab Oktober 2003 in 23 Bahnstationen die Bilder der dortigen Überwachungskameras nicht mehr nur in gefährlichen Situationen, sondern permanent aufgezeichnet werden sollen.

15.09.: **Sexuelle Übergriffe der Polizei Bremen:** Ein Bremer Polizeibeamter wird vom Dienst suspendiert, weil er 1998/99 weibliche Gefangene im Abschiebegewahrsam zu sexuellen Handlungen gezwungen haben soll. Im November werden die Ermittlungen auf weitere Beamte ausgedehnt. Am 17.11. bestätigt Polizeipräsident Eckard Mordhorst, dass aufgrund der Beschwerden einer Gefangenen bereits 1998 eine allerdings ergebnislose interne Untersuchung geführt worden war. Die Opfer sind mittlerweile alle abgeschoben. Einige der jetzt zur Debatte stehenden Übergriffe sind bereits verjährt.

16.09.: **Rosenholz-Kartei:** Die 141 Mitglieder des Berliner Abgeordnetenhauses werden anhand der sog. Rosenholz-Kartei erneut – zum zweiten Mal in zwei Jahren – auf eine frühere Stasi-Mitarbeit überprüft. Im Zusammenhang mit der Kartei, in der die Namen von 50.000 Westdeutschen mit Stasi-Kontakten verzeichnet sind, steht auch der Schriftsteller Günter Wallraff im Verdacht, für die Stasi gespitzelt zu haben.

Freispruch für Flüchtlingsberater: Das AG Berlin-Tiergarten spricht den Leiter und eine Mitarbeiterin der Berliner Beratungsstelle für Folteropfer vom Vorwurf des Widerstands gegen Vollstreckungsbeamte

frei. Ihnen war vorgeworfen worden, im November 2002 die Festnahme eines 17-jährigen Kurden behindert zu haben. Als die Polizei auf der Suche nach dem jungen Mann durch die Beratungsstelle stürmte, war dieser aus dem Fenster gesprungen und hatte lebensgefährliche Verletzungen erlitten.

17.09.: **Kohls Stasi-Unterlagen:** Das VG Berlin gibt der Bundesbeauftragten für die Stasi-Unterlagen recht. Die Akten über Ex-Kanzler dürfen wie die anderer Personen der Zeitgeschichte grundsätzlich herausgegeben werden.

18.09.: **MAD-Einsatz im Ausland:** Das Bundeskabinett verabschiedet einen Gesetzentwurf, gemäß dem der Militärische Abschirmdienst nicht mehr nur im Inland, sondern bei Auslandseinsätzen der Bundeswehr auch jenseits der bundesdeutschen Grenzen arbeiten soll.

24.09.: **Todesschuss auf Verwirrten:** Im niedersächsischen Mellendorf attackiert ein 40-Jähriger mehrere Anwohner und anschließend die zu Hilfe gerufene Polizei. Ein Polizist wird von einer Stablampe am Kopf getroffen und gibt darauf zunächst einen Warnschuss und danach mehrere Schüsse auf den Körper des offenbar verwirrten Mannes ab, der später im Krankenhaus stirbt.

25.09.: **Hartes Landfriedensbruch-Urteil:** Das AG Berlin-Tiergarten verurteilt einen in Berlin lebenden 29-jährigen Polen wegen Landfriedensbruch, schwerem Widerstand gegen Vollstreckungsbeamte, gefährlicher Körperverletzung und Beleidigung zu drei Jahren und zehn Monaten Haft. Er habe am 1. Mai 2003 Steine auf Polizisten geworfen, bei der Festnahme um sich getreten und Beamte beschimpft.

Oktober 2003

01.10.: **Frauenhäuser nicht mehr anonym:** Die Hamburger Behörde für Soziales und Familie weist die Frauenhäuser an, monatlich die Namen der wieder ausgezogenen Frauen zu melden. Die Behörde will so die tatsächliche Auslastung der Häuser, deren Konzept Anonymität ist, prüfen und die Vergabe öffentlicher Mittel besser kontrollieren.

09.10.: **Freispruch für Polizisten:** Das LG Mühlhausen (Thüringen) spricht einen Polizisten vom Vorwurf der fahrlässigen Tötung frei. Er hatte einen 30-jährigen Automaten-Knacker mit einem Schuss in den

Rücken tödlich getroffen. Das Gericht wertete den Schuss als Notwehr. (Az: 142 Js55603/02)

15.10.: **Telekommunikationsgesetz-Entwurf:** Das Bundeskabinett verabschiedet den Regierungsentwurf für ein neues Telekommunikationsgesetz. Alle Betreiber von Telekommunikationsdiensten müssen demnach die Aufstellung von Überwachungsgeräten für die strategische Fernmeldeüberwachung dulden und BND-Bediensteten sowie der Kontrollkommission des Bundestags jederzeit Zugang gewähren.

16.10.: **Geldstrafe für Aufruf zu Anti-Nazi-Demo:** Der Münchner Grünen-Stadtrat Siegfried Benker kassiert eine Geldstrafe von 150 Euro. Er hatte Ende 2002 dazu aufgerufen, sich einer Neonazi-Demonstration gegen die Wehrmachtsausstellung „friedlich entgegenzustellen".

21.10.: **Prozessauftakt in Halle**: Im Sicherheitstrakt des Justizzentrums Halle Beginnt der Prozess gegen drei 22- bis 24-jährige Magdeburger, denen die Bundesanwaltschaft Mitgliedschaft in einer terroristischen Vereinigung sowie mehrere Brandanschläge vorwirft.

24.10.: **Big Brother Award 2003:** Die diesjährigen Datenschutz-Negativ-Preise gehen u.a. an Berlins Innensenator Ehrhart Körting (SPD) wegen der von der Berliner Polizei eingesetzten „verdeckten SMS" zur Lokalisierung von Verdächtigen sowie an die Innenminister von Bayern, Niedersachsen, Rheinland-Pfalz und Thüringen für die (geplante) Einführung der präventiven Telefonüberwachung im Polizeirecht.
Folter und Auslieferung: Das BVerfG verwirft die Verfassungsbeschwerde von Pablo Elkoro gegen seine Auslieferung nach Spanien. Spanien habe den EU-Vertrag und die UN-Anti-Folterkonvention unterzeichnet, es bestehe kein Grund für die Annahme, dass Gefangene, die der Mitgliedschaft oder Unterstützung der ETA beschuldigt werden, gefoltert würden.
Urteil im Potzlow-Prozess: Das LG Neuruppin (Brandenburg) verurteilt drei Skinheads, die im Juli 2002 einen als links geltenden Schüler stundenlang gequält und dann ermordet hatten, zu 15 Jahren, acht Jahren und sechs Monaten bzw. zwei Jahren Gefängnis. Die Leiche des Schülers war erst Monate später in einer Jauchegrube gefunden worden.

25.10.: **Erstmals Schadensersatz nach Lauschangriff:** Nachdem das LG Freiburg schon 1998 die Rechtswidrigkeit des Lauschangriffs festgestellt hatte, spricht nun der BGH einer Bauernfamilie aus dem Schwarzwald Schadensersatz zu. Gestützt auf das baden-

württembergische Polizeigesetz hatte die Polizei eineinhalb Jahre lang eine Wanze in dem Bauernhof installiert. Die Familie war verdächtigt worden, zwischen 1992 und 1995 auf dem eigenen Hof sowie in Horben bei Freiburg Feuer gelegt zu haben. Der Verdacht wurde nie erhärtet.

27.10.: **Berliner Polizeitaktik 1. Mai 2004:** Polizeipräsident Dieter Glietsch stellt Pläne für den Umgang mit den Krawallen vor. Entscheidungsbefugnisse sollen stärker „nach unten" delegiert werden, zivile und uniformierte Beamte sich stärker unter die Menschen mischen.

29.10.: **Rechtsextreme Gruppe aufgelöst:** Bei einer Razzia in mehreren Städten gegen die rechtsextremistische Gruppierung „Combat 18" beschlagnahmen 300 schleswig-holsteinische Polizisten Waffen und nehmen sechs Verdächtige fest, u.a. einen Ex-NPD-Landesvorsitzenden.

30.10.: **Sicherungsverwahrung:** Der niedersächsische Landtag beschließt ein Gesetz, wonach als nicht-therapierbar geltende Straftäter nachträglich in Sicherungsverwahrung genommen werden können. Gegen ähnliche Gesetze in Sachsen-Anhalt und Bayern sind Verfassungsbeschwerden beim BVerfG anhängig.

November 2003

01.11.: **Rasterfahndung:** Brandenburgs Innenminister Jörg Schönbohm teilt mit, dass aufgrund der Rasterfahndung seit Oktober 2002 in Brandenburg rund 20.000 Personen überprüft worden sind.

02.11.: **GSG 9 im Irak**: Das BMI bestätigt, dass die Grenzschutzgruppe 9 im Irak im Einsatz ist, um Mitarbeiter des Technischen Hilfswerks, die dort das Trinkwassernetz wiederaufbauen, vor Anschlägen zu schützen.

08.11.: **Münchner Neonazis:** Der BGH erlässt Haftbefehle gegen 14 Rechtsextreme, davon elf aus der „Kameradschaft Süd". Sie werden beschuldigt, einen Sprengstoffanschlag auf die Baustelle des jüdischen Gemeindezentrums in München sowie weitere Anschläge geplant zu haben.

12.11.: **Bewährungsstrafen für Neonazis:** Wegen Mitgliedschaft in einer terroristischen Vereinigung, schwerem Landfriedensbruchs und gefährlicher Körperverletzung verurteilt das LG Dresden elf Mitglieder der 2001 verbotenen „Skinheads Sächsische Schweiz" (SSS) zu Strafen zwischen sechs Monaten bis zwei Jahren auf Bewährung.

14.11.: **Haftstrafe für Bremer Polizisten:** Das AG Frankfurt/Main verurteilt einen Polizeikommissar wegen gefährlicher Körperverletzung im Amt zu zweieinhalb Jahren Haft. Der 46-Jährige hatte bei einem Einsatz in Bad Homburg einen Obdachlosen schwer misshandelt.

17.11.: **Castor-Transport 2003:** Das niedersächsische Innenministerium gibt bekannt, dass gegen die nach Polizeiangaben 3.500 DemonstrantInnen 12.500 PolizistInnen im Einsatz waren. Der Einsatz kostete 25 Mio. Euro. 1.247 Personen habe die Polizei in Gewahrsam genommen, 255 in die Gefangenensammelstelle „Neu Tramm" gebracht. 85 Strafverfahren wurden eingeleitet.

18.11.: **Auslieferung an USA:** Zwei in den USA unter Terrorverdacht stehende und in Deutschland verhaftete Jemeniten werden ausgeliefert, nachdem das BVerfG ihre Verfassungsbeschwerde zurückgewiesen hat.

21.11.: **Freispruch für Berliner Polizisten:** Das LG Berlin spricht zwei Beamte vom Vorwurf der Misshandlung eines aus der Türkei stammenden Kameramannes frei. Als Folge eines Polizeieinsatzes in der Nacht zum 1. Mai 2000 hatte der Mann einen Nasenbeinbruch und ein Schädelhirntrauma erlitten. Die Vorfälle seien nicht mehr aufzuklären. Der Kameramann wurde seinerseits vom Vorwurf des Widerstandes freigesprochen.

22.11.: **Innenminister wollen abschieben:** Die Innenministerkonferenz ist sich einig, ab 2004 Flüchtlinge aus Afghanistan „zurückzuführen". Auch irakische Flüchtlinge sollen gehen, wobei die „freiwillige Heimführung" Vorrang habe.

26.11.: **Urteil gegen Al Tawhid-Mitglied:** Das Oberlandesgericht Düsseldorf verurteilt den Palästinenser Shadi Abdella wegen Mitgliedschaft in einer terroristischen Vereinigung zu vier Jahren Haft. Der 27-Jährige hatte zugegeben, verschiedene Anschläge in Düsseldorf und Berlin geplant zu haben. Nach seiner Verhaftung 2002 hatte Abdella vier Komplizen beschuldigt, was das Gericht in seinem Urteil honorierte. Bei der Urteilsverkündung warb der Vorsitzende für die Wiedereinführung der 1999 ausgelaufenen Kronzeugenregelung.

Marion Knorr ist Politikwissenschaftlerin und Redaktionsmitglied von Bürgerrechte & Polizei/CILIP.

Literatur

Zum Schwerpunkt

Seit wir uns 1998 in zwei Schwerpunktheften (CILIP 60 und 61, H. 2 und 3/1998) unter der Überschrift „Überwachungstechnologien“ mit einem Aspekt des Themas „Polizei und Technik“ beschäftigten, haben sich die technischen Möglichkeiten wie ihr Gebrauch innerhalb der Polizeien rasant weiterentwickelt. Dieser schnelle Wandel, der Einzug fortgeschrittener Techniken in die meisten polizeilichen Arbeitsbereiche und die komplizierten Funktionsweisen sind vermutlich verantwortlich dafür, dass es weder eine Bestandsaufnahme der polizeilichen Techniknutzung in Deutschland gibt, noch eine aktuelle Analyse im Hinblick darauf, wie die modernen technischen/technologischen Potentiale die Polizei selbst und ihre gesellschaftliche Rolle verändern. Angesichts dieser Literatur- und Forschungslage beinhalten auch die folgenden Hinweise nur Teile eines unvollständigen Puzzles. Auf die Literatur zur Entwicklung „intelligenter“ und „weniger tödlicher“ Waffen haben wir (aus Platzgründen) verzichtet. Veröffentlichungen, die sich auf einzelne, in diesem Heft genauer vorgestellte Techniken beziehen, sind in den Fußnoten der entsprechenden Artikel aufgeführt.

Sack, Fritz; Nogala, Detlef; Lindenberg, Michael: *Social Control Technologies. Aspekte und Konsequenzen des Technikeinsatzes bei Instanzen strafrechtlicher Sozialkontrolle im nationalen und internationalen Kontext, Hamburg 1997 (unveröffentlichter Forschungsbericht)*
Nogala, Detlef: *Social Control Technologies. Verwendungsgrammatiken, Systematisierung und Problemfelder technisierter sozialer Kontrollarrangements, Berlin 1998 (Dissertation, nur als Microfiche in Bibliotheken erhältlich)*
Beide Schriften, die aus einem von der VW-Stiftung finanzierten Forschungsprojekt resultierten, sind für alle unverzichtbar, die sich mit „Polizei und Technik“ beschäftigen wollen. Sie geben einen Überblick über die Einsatzbereiche der Technologien sozialer Kontrolle – von der Alarmierung bis zur elektronischen Fußfessel, von der Datenverarbeitung bis

zur Bewaffnung. Obwohl die Darstellungen im Einzelnen von der technischen Entwicklung überholt sind, ist deren systematische Aufbereitung nach wie vor lehrreich. Zudem beschränken sich die Arbeiten nicht auf die technische Ebene, sondern sie untersuchen die gesellschaftlichen Folgen technikgestützter Sozialkontrolle.

Hetger, Erwin: *Chancen und Risiken neuer Techniken, in: Die Polizei 94. Jg., 2003, H. 12, S. 333-337*
Der aktuelle Aufsatz des baden-württembergischen Landespolizeipräsidenten steht symptomatisch für die polizeiliche Wahrnehmung des „Technik-Problems". Ausgangspunkt bilden die Kriminalitätsgefahren, die den neuen (insbesondere) Kommunikationstechnologien innewohnen: neue Delikte und neue Begehungsformen durch die Möglichkeiten des Internet. Verschlüsselungsprogramme und moderne Internetzugänge stellten die Polizeien vor erhebliche Ermittlungsprobleme. Diesen „Risiken" werden die in der technischen Entwicklung liegenden Chancen für die Polizei gegenübergestellt: Diese lägen, so Hetger, „auf nahezu allen Ebenen wie bspw. im Bereich der Prävention, Repression, Öffentlichkeitsarbeit ... Aus- und Fortbildung". Einzelne Techniken werden im Folgenden kurz vorgestellt: DNA-Analytik, Sicherung digitaler Spuren, biometrische Identifizierung, Videoüberwachung, Kfz-Kennzeichenlesesysteme, Fahndungen und Anzeigenerstattung per Internet. Wo erforderlich, müsse der Gesetzgeber die rechtlichen Bestimmungen neu fassen, um die technischen Potentiale voll nutzen zu können. Wie weit die technischen Möglichkeiten reichen, wird an der kurzen Aufzählung „digitaler Spuren" deutlich: Diese fielen nicht allein im Internet an, sondern auch in Telefonapparaten, in digitalen Video- und Fotokameras, im Scheck- und Kreditkartenverfahren, in der modernen Fahrzeugtechnik ... Dass den „Spurenverursachern" entweder ihre Spuren nicht bewusst seien oder ihnen das Know-how fehle, sie zu beseitigen, sei „für die Polizei ein glücklicher Umstand, den es für die Ermittlungen zu nutzen gilt".

Knecht, Wolfgang: *Modernisierung der technischen Ausstattung der Polizei Baden-Württemberg, in: Deutsches Polizeiblatt 20. Jg., 2002, H. 5, S. 32-35*
In diesem Beitrag wird das „Technik-Zukunftsprogramm" beschrieben, durch das die technische Ausstattung und Ausrüstung der baden-württembergischen Polizei bis zum Jahr 2005 „umfassend und nachhaltig" erneuert werden soll. Das auf sieben Jahre angelegte Investitionspro-

gramm hat einen Umfang von 341 Mio. Euro. Durch diese Mittel werden neue Autos, Boote und Hubschrauber angeschafft. Über 10.000 Schutzwesten und rund 25.000 neue Pistolen werden gekauft. Im Bereich der Datenverarbeitung werden alle Dienststellen „mit einer Vollverkabelung und mit über 14.000 leistungsfähigen PC ausgestattet". Zudem sieht das Programm die Ausweitung der DNA-Analysekapazitäten vor, die Modernisierung der Ausstattungen von SEK und MEK etc.

Deutsches Polizeiblatt 2001, H. 5: *Moderne Polizeitechnik (Schwerpunkt)*
Das Heft gibt einen interessanten Überblick über den Einzug der Technik in die Polizeiarbeit in der Bundesrepublik. In einzelnen Beiträgen werden die Planungen zu Inpol-neu und zur Einführung des Digitalfunks vorgestellt. Die Videoüberwachung in Leipzig, die DNA-Analysedatei, die Wärmebildgeräte des Bundesgrenzschutzes oder die „Polizeihubschrauber der neuen Generation" werden ebenso vorgestellt wie verschiedene EDV-Anwendungen. Wie sehr die Kommunikationstechnik die Polizeiarbeit verändert, wird in den Berichten über das „Berliner Befehlsstellen Informationssystem" (BEBIS), das der Bewältigung von Groß- und Sonderlagen dient, oder über das Münchener „Geographische Lage-/Analyse-/Darstellungs- und Informationssystem (GLADIS) deutlich. In der Darstellung des sächsischen Systems der „Integrierten Vorgangsbearbeitung" (IVO) wird deutlich, dass die Datenverarbeitung die polizeiliche Arbeitsorganisation erheblich verändern wird. Dies verspricht zum einen Rationalisierungsgewinne (Bereinigung von Formularen, Wegfall von Mehrfacherfassungen), schafft zum anderen aber auch die Voraussetzungen dafür, verschiedene Datenbestände in Sekundenschnelle und per Knopfdruck zusammenzuführen.

Dewald, Michael: *Die Datenbank ViCLAS, in: Kriminalistik 56. Jg., 2002, H. 4, S. 248-255*
Seit Juni 2000 wird beim Bundeskriminalamt die Verbunddatei ViCLAS betrieben. Die Abkürzung steht für „Violent Crime Linkage Analysis System" (Analysesystem zur Zusammenführung von Gewaltverbrechen). Das System wurde von der kanadischen Polizei entwickelt und seit der zweiten Hälfte der 90er Jahre von einigen Landespolizeien (Bayern, Baden-Württemberg, Brandenburg) und dem Bundeskriminalamt eingesetzt. ViCLAS dient dazu, Wiederholungstäter oder serienmäßig begangene Taten auch dann zu entdecken, wenn sie an verschiedenen Orten

(national oder international) begangen wurden. Das System ist für Ermittlungen im Bereich der gewalthaften Sexualdelikte ausgelegt; es stellt ein Hilfsmittel der „operativen Fallanalyse“ dar. In ViCLAS werden Meldungen durch ein umfangreiches Multiple-Choice-Verfahren in vollständige recherchierbare Datenfelder übertragen. Eineinhalb Jahre nach ihrer Einrichtung waren knapp 5.700 Fälle in die Bundesdatei eingestellt. „Trotz kleinem Datenbestand“ kam es, so Dewald, „überraschenderweise ... bereits zu mehreren Fallverknüpfungen, die durch anschließende Ermittlungen bestätigt werden konnten“.

Luckey, Horst; Krusenbaum, Bernd: *„FINDUS“ effektiviert Analyse und Auswertung, in: Polizei – heute 31. Jg., 2002, H. 5, S. 199-202*
Während die ViCLAS-Methode für jedes Delikt spezifiziert werden muss, versprechen andere Systeme generelle Einsetzbarkeit. So wurde FINDUS („Fallinformationen durchsuchen mit System“) im Auftrag des nordrhein-westfälischen Innenministeriums entwickelt. Ursprünglich für die Spezialdienststellen zur Bekämpfung Organisierter Kriminalität gedacht, können mit FINDUS komplexe Informationen ausgewertet und Zusammenhänge erkannt werden. Im Unterschied zu ViCLAS, das der (reaktiven) Fallaufklärung dient, kann FINDUS auch für die Strategien der (proaktiven) Verdachtschöpfung und -verdichtung eingesetzt werden. Auch dieses Landesprogramm fußt auf dem Prinzip der Einmalerfassung, so dass es über Schnittstellen mit anderen Daten (Vorgangsbearbeitung, Tagebuchführung) verbunden ist. In der Regel werden die FINDUS-Dateien von den lokalen Polizeibehörden geführt; die Sachbearbeiter entscheiden, ob die Daten zusätzlich auf dem FINDUS-Landesserver abgelegt werden sollen. Auch der kriminalpolizeiliche Meldedienst wird über das Programm abgewickelt. Da Analyse und Auswertung im Zentrum von FINDUS stehen, werden harte und weiche Daten gespeichert. „Weiche“ Daten sind Informationen, deren kriminalistische Relevanz fraglich ist;. es kann sich dabei um Bekannte von Verdächtigen oder um Telefonnummern Unbekannter handeln. Der praktische Vorteil von FINDUS besteht darin, dass das Programm die grafische Darstellung von Beziehungen erlaubt, die zwischen verschiedenen Daten bestehen. Mit Hilfe von FINDUS seien die Daten der Rasterfahndung nach „Schläfern“ zusammengeführt worden; der abgebildete „Screeshot“ illustriert die Möglichkeiten des Programms. Beim Staatsschutz wurde im Sommer 2002 die Anwendung TAURUS/FINDUS vorbereitet. „TAURUS“ steht für „TKÜ-Auswertung/Recherche und Unterstützung von Ermittlungen“

(TKÜ = Telekommunikationsüberwachung). Mit TAURUS sollen digitale Gesprächsaufzeichnungen, Protokolle und Verbindungsdaten automatisch zusammengeführt werden.

Neuerscheinung

Gössner, Rolf: *Geheime Informanten. V-Leute des Verfassungsschutzes: Kriminelle im Dienste des Staates, München (Knaur Taschenbuch) 2003, 316 S., EUR 12,90*

Die ersten 150 Seiten seiner Abrechnung mit den Kriminellen im verfassungsschützerischen Staats-Dienst widmet Gössner einzelnen V-Leuten: ihren Einsatzgebieten, ihren (kriminellen) Leistungen, ihrer Biografie etc.: von niedersächsischen Bombenbeschaffern in den 70er Jahren bis zu den Aktivisten der Neonazi-Musikszene Ende der 90er, von dem Kampfsportlehrer aus Solingen bis zum gewöhnlichen Schläger aus der mecklenburgischen Provinz. Überall deckt Gössner das Zusammenspiel zwischen gescheiterten Existenzen, fragwürdigen Typen und/oder verurteilten Straftätern und den Verfassungsschutzämtern auf. Der Skandal, das machen diese Schilderungen deutlich, besteht nicht allein in den jeweiligen Fällen, sondern in dem System, das sie notwendig produziert: in der Logik der Infiltration, der sich die „Ämter“ verschrieben haben.

Im zweiten Teil des Buches stellt Gössner den Umgang der Apparate mit ihren „Vertrauens“-Leuten dar – von der Anwerbung über die Bezahlung, ihrer „Führung“ und ihres Schutzes vor dem „Verbrennen“. Die Zusammenarbeit mit dem kriminellen Milieu ist die Voraussetzung der V-Mann-Arbeit; und die mangelnde Kontrolle dieser zwielichtigen Agenten ist ihre unausweichliche Folge. Leider taucht der polizeiliche V-Leute-Einsatz, der dieselben Probleme produziert, nur am Rande auf. Das Thema wäre sicher eine eigene Untersuchung wert. Die verheerenden Folgen der Unterwanderungsarbeit zeigt Gössner erneut im dritten Teil am Beispiel der V-Leute aus den Reihen der Reps und der NPD.

In seinen abschließenden Bemerkungen („reformieren oder abwikkeln“) ist Gössner die Sympathie für das Abwickeln der Verfassungsschutzämter deutlich anzumerken. Aber sein Plädoyer läuft auf moderate Reformen hinaus: der V-Mann-Einsatz als „Ultma Ratio“, die Überwachung von Parteien nur nach Anordnung durch ein Verwaltungsgericht, parlamentarische Berichtspflichten etc. Ungeachtet dieser „Filigranarbeit beim Versuch einer rechtsstaatlichen Zähmung ... könnte die V-Mann-Affäre möglicherweise der Überlegung Auftrieb verschaffen, diesen In-

landsgeheimdienst gänzlich aufzulösen“. Ein Konjunktiv und ein „möglicherweise“ zu viel.
(sämtlich: Norbert Pütter)

Summaries

Technologies of repression and the compelling necessity to politicise them

by Wolf-Dieter Narr

From the moment on that the police developed as a force out of the military during the 19th century, its specific technical equipment has played a central role. At the end of the 1960's, informational and violent techniques in the fight against crime, the pacification of riots and criminal prosecution, became technologies that fundamentally transformed the police force. In view of the technologically refined interventions, the control mechanisms of law and representative democracy are failing. Now the time has come to redefine human rights in a more differentiated manner in order to grasp and communicate the increasingly sublime violations of rights.

INPOL-new: Informationalising every day police work

by Heiner Busch

After more than 10 years of planning and development and after a far-reaching failure of the original plans and a modest new start, the first stage of the new common information system of the German police went online in August 2003. Together with the journal and reports systems that were introduced at the regional level, INPOL-new will lead to a far-reaching computerisation, also of everyday police work.

Digital radio also costs money

by Stephan Stolle

Digital radio is not only tap-proof but also allows for direct access to police databases. Since the 1990's, the EU has been working on common standards for digital radio. However, since France decided in a solo effort to go for the Tetrapol-Standard developed by Matra, the EU-wide harmony is over. There will also be no German nation-wide digital radio system in the near future as at the end of 2002, the regional and federal finance ministers have put a halt to the 9 thousand million Euro project.

DNA-Analysis

by Detlef Nogala

Forensic DNA-analysis, often delusively called 'genetic fingerprinting', has reached a status within police practice, that has lead to political initiatives arguing for a broadened use of this technology. The article discusses the technical development of forensic DNA-analysis and DNA-databases with view to recent criminological and political reasoning. It points out that there is a strong tendency to register more delinquent populations in order to get more 'hits'. Civil libertarian arguments seem to be in the defensive.

Biometrics Boom after 11 September 2001

by Jonathan P. Aus

Since 11 September 2001, the US and the EU are driving the systematic collection and exchange of biometric data forward. In the area of biometric travel documents and border controls, transatlantically agreed standards are now within reach. The US are currently developing a system called US-VISIT, the EU wants to fit the Visa Information System (VIS) and the Schengen Information System (SIS) with biometric data after it already introduced such a system with Eurodac one year ago.

Automatic number plate reading

by Daniel Boos

The use of Automatic Number Plate Reading (ANPR) systems began in the UK in the 1990's. Meanwhile the technology has spread to the continent. ANPR systems "read" the video camera transmitted picture of a number plate, transform it into text form and thereby enable further processing, that is the comparison with a database or the creation of movement patterns.

"Non-lethal" weapons for wars and internal operations

by Olaf Arndt and David Artichouk

In May 2003, the Fraunhofer Institute for Chemical Technology organised a conference for manufacturers and users of so called non-lethal weapons. The conference showed that the allegedly harmless weapons could be the future for military operations in the "War against Terrorism"

as well as for special police units. There seem to be no limits to the repressive imagination here.

Mutual assistance and extradition agreements with the USA

by Hartmut Wächtler

Soft formulations and far-reaching abandonment of legal protection and data protection possibilities characterise the most recent agreements which the EU has made with the US: the agreement on exchange of personal data with Europol as well as the Conventions on mutual assistance in criminal matters and extradition. The bilateral agreement on mutual assistance between Germany and the US also fails to provide real barriers that would prevent a cooperation with the US military tribunals.

Bad times for civil liberties in the USA

by Clemens Arzt

The USA are fighting their "War against Terrorism" internally as well. The USA Patriot Act is an extensive an untransparent law. It creates new criminal offences (terrorism definition). It blurs the separation of criminal prosecution and secret services which was introduced after the Watergate Scandal. In particular, it has introduced powers to arrest migrants without proper proceedings.

Playing down the surveillance of telecommunications

by Norbert Pütter

By order of the Federal Ministry of Justice, the Freiburg Max-Planck-Institute drew up a report on surveillance of telecommunications in Germany. The report increases public knowledge and confirms known facts, but instead of providing a critique guided by constitutional rights, it legitimises the existing practise of surveillance, which was positively received by the minister of justice.